TigerSwitch 10/100/1000

Gigabit Ethernet Switch

- 12 1000BASE-X SFP ports
- 4 RJ45 ports shared with 4 SFP transceiver slots
- Non-blocking switching architecture
- Support for a redundant power unit
- Spanning Tree Protocol
- Up to six LACP or static 4-port trunks
- Layer 2/3/4 CoS support through four priority queues
- Full support for VLANs with GVRP
- IGMP multicast filtering and snooping
- Support for jumbo frames up to 9 KB
- Manageable via console, Web, SNMP/RMON

SMC® Networks

Management Guide

SMC8612XL3

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

TigerSwitch 10/100/1000 Management Guide

From SMC's Tiger line of feature-rich workgroup LAN solutions

SMC® Networks
38 Tesla
Irvine, CA 92618
Phone: (949) 679-8000

October 2003
Pub. # 150200039900A

Downloaded from www.Manualslib.com manuals search engine

Information furnished by SMC Networks, Inc. (SMC) is believed to be accurate and reliable. However, no responsibility is assumed by SMC for its use, nor for any infringements of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent or patent rights of SMC. SMC reserves the right to change specifications at any time without notice.

Copyright © 2003 by
SMC Networks, Inc.
38 Tesla
Irvine, CA 92618
All rights reserved. Printed in Taiwan

Trademarks:

SMC is a registered trademark; and EZ Switch, TigerStack and TigerSwitch are trademarks of SMC Networks, Inc. Other product and company names are trademarks or registered trademarks of their respective holders.

Downloaded from www.Manualslib.com manuals search engine

LIMITED WARRANTY

Limited Warranty Statement: SMC Networks, Inc. ("SMC") warrants its products to be free from defects in workmanship and materials, under normal use and service, for the applicable warranty term. All SMC products carry a standard 90-day limited warranty from the date of purchase from SMC or its Authorized Reseller. SMC may, at its own discretion, repair or replace any product not operating as warranted with a similar or functionally equivalent product, during the applicable warranty term. SMC will endeavor to repair or replace any product returned under warranty within 30 days of receipt of the product.

The standard limited warranty can be upgraded to a Limited Lifetime* warranty by registering new products within 30 days of purchase from SMC or its Authorized Reseller. Registration can be accomplished via the enclosed product registration card or online via the SMC web site. Failure to register will not affect the standard limited warranty. The Limited Lifetime warranty covers a product during the Life of that Product, which is defined as the period of time during which the product is an "Active" SMC product. A product is considered to be "Active" while it is listed on the current SMC price list. As new technologies emerge, older technologies become obsolete and SMC will, at its discretion, replace an older product in its product line with one that incorporates these newer technologies. At that point, the obsolete product is discontinued and is no longer an "Active" SMC product. A list of discontinued products with their respective dates of discontinuance can be found at: **http://www.smc.com/index.cfm?action=customer_service_warranty**.

All products that are replaced become the property of SMC. Replacement products may be either new or reconditioned. Any replaced or repaired product carries either a 30-day limited warranty or the remainder of the initial warranty, whichever is longer. SMC is not responsible for any custom software or firmware, configuration information, or memory data of Customer contained in, stored on, or integrated with any products returned to SMC pursuant to any warranty. Products returned to SMC should have any customer-installed accessory or add-on components, such as expansion modules, removed prior to returning the product for replacement. SMC is not responsible for these items if they are returned with the product.

Customers must contact SMC for a Return Material Authorization number prior to returning any product to SMC. Proof of purchase may be required. Any product returned to SMC without a valid Return Material Authorization (RMA) number clearly marked on the outside of the package will be returned to customer at customer's expense. For warranty claims within North America, please call our toll-free customer support number at (800) 762-4968. Customers are responsible for all shipping charges from their facility to SMC. SMC is responsible for return shipping charges from SMC to customer.

WARRANTIES EXCLUSIVE: IF AN SMC PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, CUSTOMER'S SOLE REMEDY SHALL BE REPAIR OR REPLACEMENT OF THE PRODUCT IN QUESTION, AT SMC'S OPTION. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OR CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. SMC NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER

Downloaded from www.Manualslib.com manuals search engine

LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS. SMC SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD.

LIMITATION OF LIABILITY: IN NO EVENT, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), SHALL SMC BE LIABLE FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE, LOSS OF BUSINESS, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCTS, EVEN IF SMC OR ITS AUTHORIZED RESELLER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME STATES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES OR THE LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES FOR CONSUMER PRODUCTS, SO THE ABOVE LIMITATIONS AND EXCLUSIONS MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, WHICH MAY VARY FROM STATE TO STATE. NOTHING IN THIS WARRANTY SHALL BE TAKEN TO AFFECT YOUR STATUTORY RIGHTS.

* SMC will provide warranty service for one year following discontinuance from the active SMC price list. Under the limited lifetime warranty, internal and external power supplies, fans, and cables are covered by a standard one-year warranty from date of purchase.

SMC Networks, Inc.
38 Tesla
Irvine, CA 92618

Downloaded from www.Manualslib.com manuals search engine

CONTENTS

Chapter 1: Introduction 1-1

Key Features 1-1
Description of Software Features 1-2
System Defaults 1-7

Chapter 2: Initial Configuration 2-1

Connecting to the Switch 2-1
Configuration Options 2-1
Required Connections 2-2
Remote Connections 2-3
Basic Configuration 2-3
Console Connection 2-3
Setting Passwords 2-4
Setting an IP Address 2-4
Manual Configuration 2-4
Dynamic Configuration 2-5
Enabling SNMP Management Access 2-6
Community Strings 2-6
Trap Receivers 2-7
Saving Configuration Settings 2-7
Managing System Files 2-8

Chapter 3: Configuring the Switch 3-1

Using the Web Interface 3-1
Navigating the Web Browser Interface 3-2
Home Page 3-2
Configuration Options 3-2
Panel Display 3-3
Main Menu 3-3
Basic Configuration 3-10
Displaying System Information 3-10
Displaying Switch Hardware/Software Versions 3-11
Displaying Bridge Extension Capabilities 3-12
Setting the Switch's IP Address 3-14
Manual Configuration 3-15

Downloaded from www.Manualslib.com manuals search engine

Using DHCP/BOOTP 3-16
Managing Firmware 3-17
Downloading System Software from a Server 3-17
Saving or Restoring Configuration Settings 3-18
Downloading Configuration Settings from a Server 3-19
Configuring Event Logging 3-20
System Log Configuration 3-20
Remote Log Configuration 3-21
Displaying Log Messages 3-23
Resetting the System 3-23
Setting the System Clock 3-24
Configuring SNTP 3-25
Setting the Time Zone 3-26
Simple Network Management Protocol 3-26
Setting Community Access Strings 3-27
Specifying Trap Managers and Trap Types 3-28
Filtering Addresses for SNMP Client Access 3-29
User Authentication 3-30
Configuring the Logon Password 3-30
Configuring Local/Remote Logon Authentication 3-31
Configuring HTTPS 3-34
Replacing the Default Secure-site Certificate 3-35
Configuring the Secure Shell 3-35
Generating the Host Key Pair 3-37
Configuring the SSH Server 3-39
Configuring Port Security 3-40
Configuring 802.1x Port Authentication 3-42
Displaying 802.1x Global Settings 3-43
Configuring 802.1x Global Settings 3-45
Configuring Port Authorization Mode 3-46
Displaying 802.1x Statistics 3-47
Filtering Management Access 3-48
Access Control Lists 3-50
Configuring Access Control Lists 3-50
Setting the ACL Name and Type 3-51
Configuring a Standard IP ACL 3-52
Configuring an Extended IP ACL 3-53

Downloaded from www.Manualslib.com manuals search engine

Configuring a MAC ACL 3-55
Configuring ACL Masks 3-57
Specifying the Mask Type 3-57
Configuring an IP ACL Mask 3-58
Configuring a MAC ACL Mask 3-60
Binding a Port to an Access Control List 3-61
Port Configuration 3-62
Displaying Connection Status 3-62
Configuring Interface Connections 3-65
Creating Trunk Groups 3-67
Statically Configuring a Trunk 3-68
Enabling LACP on Selected Ports 3-69
Configuring LACP Parameters 3-71
Displaying LACP Port Counters 3-73
Displaying LACP Settings and Status for the Local Side . 3-74
Displaying LACP Settings and Status for the Remote Side . . . 3-77
Setting Broadcast Storm Thresholds 3-78
Configuring Port Mirroring 3-80
Configuring Rate Limits 3-81
Showing Port Statistics 3-82
Address Table Settings 3-86
Setting Static Addresses 3-86
Displaying the Address Table 3-87
Changing the Aging Time 3-88
Spanning Tree Algorithm Configuration 3-88
Displaying Global Settings 3-89
Configuring Global Settings 3-92
Displaying Interface Settings 3-96
Configuring Interface Settings 3-99
Configuring Multiple Spanning Trees 3-101
Displaying Interface Settings for MSTP 3-104
Configuring Interface Settings for MSTP 3-107
VLAN Configuration 3-108
Overview 3-108
Assigning Ports to VLANs 3-109
Forwarding Tagged/Untagged Frames 3-111

Downloaded from www.Manualslib.com manuals search engine

Enabling or Disabling GVRP (Global Setting) 3-111
Displaying Basic VLAN Information 3-111
Displaying Current VLANs 3-112
Creating VLANs 3-114
Adding Static Members to VLANs (VLAN Index) 3-115
Adding Static Members to VLANs (Port Index) 3-116
Configuring VLAN Behavior for Interfaces 3-117
Configuring Private VLANs 3-120
Enabling Private VLANs 3-120
Configuring Uplink and Downlink Ports 3-121
Configuring Protocol-Based VLANs 3-121
Configuring Protocol Groups 3-122
Mapping Protocols to VLANs 3-122
Class of Service Configuration 3-124
Setting the Default Priority for Interfaces 3-124
Mapping CoS Values to Egress Queues 3-126
Selecting the Queue Mode 3-128
Setting the Service Weight for Traffic Classes 3-128
Mapping Layer 3/4 Priorities to CoS Values 3-130
Selecting IP Precedence/DSCP Priority 3-130
Mapping IP Precedence 3-131
Mapping DSCP Priority 3-132
Mapping IP Port Priority 3-134
Mapping CoS Values to ACLs 3-135
Changing Priorities Based on ACL Rules 3-136
Multicast Filtering 3-138
IGMP Protocol 3-138
Layer 2 IGMP (Snooping and Query) 3-139
Configuring IGMP Snooping and Query Parameters . . . 3-140
Displaying Interfaces Attached to a Multicast Router . . 3-141
Specifying Static Interfaces for a Multicast Router 3-142
Displaying Port Members of Multicast Services 3-144
Assigning Ports to Multicast Services 3-145
Layer 3 IGMP (Query used with Multicast Routing) 3-146
Configuring IGMP Interface Parameters 3-146
Displaying Multicast Group Information 3-149
Configuring Domain Name Service 3-150

Downloaded from www.Manualslib.com manuals search engine

Configuring General DNS Server Parameters 3-150
Configuring Static DNS Host to Address Entries 3-152
Displaying the DNS Cache 3-154
Dynamic Host Configuration Protocol 3-155
Configuring DHCP Relay Service 3-155
Configuring the DHCP Server 3-156
Enabling the Server, Setting Excluded Addresses 3-157
Configuring Address Pools 3-158
Displaying Address Bindings 3-162
Configuring Router Redundancy 3-163
Virtual Router Redundancy Protocol 3-164
Configuring VRRP Groups 3-164
Displaying VRRP Global Statistics 3-168
Displaying VRRP Group Statistics 3-169
Hot Standby Router Protocol 3-170
Configuring HSRP Groups 3-170
IP Routing 3-176
Overview 3-176
Initial Configuration 3-176
IP Switching 3-177
Routing Path Management 3-178
Routing Protocols 3-178
Basic IP Interface Configuration 3-179
Configuring IP Routing Interfaces 3-180
Address Resolution Protocol 3-182
Proxy ARP 3-182
Basic ARP Configuration 3-183
Configuring Static ARP Addresses 3-184
Displaying Dynamically Learned ARP Entries 3-185
Displaying Local ARP Entries 3-187
Displaying ARP Statistics 3-188
Displaying Statistics for IP Protocols 3-189
IP Statistics 3-189
ICMP Statistics 3-190
UDP Statistics 3-192
TCP Statistics 3-193
Configuring Static Routes 3-194

Downloaded from www.Manualslib.com manuals search engine

Displaying the Routing Table 3-195
Configuring the Routing Information Protocol 3-196
Configuring General Protocol Settings 3-197
Specifying Network Interfaces for RIP 3-199
Configuring Network Interfaces for RIP 3-200
Displaying RIP Information and Statistics 3-203
Configuring the Open Shortest Path First Protocol 3-206
Configuring General Protocol Settings 3-207
Configuring OSPF Areas 3-210
Configuring Area Ranges (Route Summarization for ABRs) . . 3-213
Configuring OSPF Interfaces 3-215
Configuring Virtual Links 3-219
Configuring Network Area Addresses 3-221
Configuring Summary Addresses (for External AS Routes) . . . 3-223
Redistributing External Routes 3-224
Configuring NSSA Settings 3-225
Displaying Link State Database Information 3-227
Displaying Information on Border Routers 3-229
Displaying Information on Neighbor Routers 3-230
Multicast Routing 3-231
Configuring Global Settings for Multicast Routing 3-231
Displaying the Multicast Routing Table 3-232
Configuring DVMRP 3-234
Configuring Global DVMRP Settings 3-234
Configuring DVMRP Interface Settings 3-237
Displaying Neighbor Information 3-239
Displaying the Routing Table 3-240
Configuring PIM-DM 3-241
Configuring Global PIM-DM Settings 3-241
Configuring PIM-DM Interface Settings 3-242
Displaying Interface Information 3-244
Displaying Neighbor Information 3-245

Chapter 4: Command Line Interface 4-1

Using the Command Line Interface 4-1

Downloaded from www.Manualslib.com manuals search engine

Accessing the CLI 4-1
Console Connection 4-1
Telnet Connection 4-1
Entering Commands 4-3
Keywords and Arguments 4-3
Minimum Abbreviation 4-3
Command Completion 4-3
Getting Help on Commands 4-3
Showing Commands 4-4
Partial Keyword Lookup 4-5
Negating the Effect of Commands 4-5
Using Command History 4-5
Understanding Command Modes 4-6
Exec Commands 4-6
Configuration Commands 4-7
Command Line Processing 4-9
Command Groups 4-10
Line Commands 4-11
line 4-11
login 4-12
password 4-13
exec-timeout 4-14
password-thresh 4-14
silent-time 4-15
databits 4-16
parity 4-16
speed 4-17
stopbits 4-17
disconnect 4-18
show line 4-18
General Commands 4-19
enable 4-19
disable 4-20
configure 4-21
show history 4-21
reload 4-22
end 4-22

Downloaded from www.Manualslib.com manuals search engine

exit 4-23
quit 4-23
System Management Commands 4-24
Device Designation Commands 4-24
prompt 4-24
hostname 4-25
User Access Commands 4-25
username 4-25
enable password 4-26
IP Filter Commands 4-27
management 4-27
show management 4-28
Web Server Commands 4-29
ip http port 4-29
ip http server 4-30
ip http secure-server 4-30
ip http secure-port 4-31
Secure Shell Commands 4-32
ip ssh server 4-34
ip ssh timeout 4-35
ip ssh authentication-retries 4-36
ip ssh server-key size 4-36
delete public-key 4-37
ip ssh crypto host-key generate 4-37
ip ssh crypto zeroize 4-38
ip ssh save host-key 4-38
show ip ssh 4-39
show ssh 4-39
show public-key 4-40
Event Logging Commands 4-41
logging on 4-41
logging history 4-42
logging host 4-43
logging facility 4-43
logging trap 4-44
clear logging 4-44
show logging 4-45

Downloaded from www.Manualslib.com manuals search engine

SMTP Alert Commands 4-46
logging sendmail host 4-47
logging sendmail level 4-47
logging sendmail source-email 4-48
logging sendmail destination-email 4-48
logging sendmail 4-49
show logging sendmail 4-49
Time Commands 4-50
sntp client 4-50
sntp server 4-51
sntp poll 4-52
sntp broadcast client 4-52
show sntp 4-53
clock timezone 4-53
calendar set 4-54
show calendar 4-54
System Status Commands 4-55
show startup-config 4-55
show running-config 4-56
show system 4-58
show users 4-59
show version 4-59
Frame Size Commands 4-60
jumbo frame 4-60
Flash/File Commands 4-61
copy 4-61
delete 4-63
dir 4-64
whichboot 4-65
boot system 4-65
Authentication Commands 4-66
Authentication Sequence 4-66
authentication login 4-66
RADIUS Client 4-67
radius-server host 4-67
radius-server port 4-68
radius-server key 4-68

Downloaded from www.Manualslib.com manuals search engine

radius-server retransmit 4-69
radius-server timeout 4-69
show radius-server 4-69
TACACS+ Client 4-70
tacacs-server host 4-70
tacacs-server port 4-71
tacacs-server key 4-71
show tacacs-server 4-71
Port Security Commands 4-72
port security 4-72
802.1x Port Authentication 4-74
authentication dot1x default 4-74
dot1x default 4-75
dot1x max-req 4-75
dot1x port-control 4-76
dot1x operation-mode 4-76
dot1x re-authenticate 4-77
dot1x re-authentication 4-77
dot1x timeout quiet-period 4-78
dot1x timeout re-authperiod 4-78
dot1x timeout tx-period 4-79
show dot1x 4-79
Access Control List Commands 4-82
IP ACLs 4-83
access-list ip 4-84
permit, deny (Standard ACL) 4-85
permit, deny (Extended ACL) 4-86
show ip access-list 4-88
access-list ip mask-precedence 4-88
mask (IP ACL) 4-89
show access-list ip mask-precedence 4-92
ip access-group 4-93
show ip access-group 4-93
map access-list ip 4-94
show map access-list ip 4-95
match access-list ip 4-95
show marking 4-96

Downloaded from www.Manualslib.com manuals search engine

MAC ACLs 4-97
access-list mac 4-97
permit, deny (MAC ACL) 4-98
show mac access-list 4-99
access-list mac mask-precedence 4-100
mask (MAC ACL) 4-101
show access-list mac mask-precedence 4-103
mac access-group 4-103
show mac access-group 4-104
map access-list mac 4-104
show map access-list mac 4-105
match access-list mac 4-105
ACL Information 4-106
show access-list 4-106
show access-group 4-107
SNMP Commands 4-107
snmp-server community 4-108
snmp-server contact 4-108
snmp-server location 4-109
snmp-server host 4-109
snmp-server enable traps 4-110
snmp ip filter 4-111
show snmp 4-112
DHCP Commands 4-113
DHCP Client 4-113
ip dhcp client-identifier 4-113
ip dhcp restart client 4-114
DHCP Relay 4-115
ip dhcp restart relay 4-115
ip dhcp relay server 4-116
DHCP Server 4-117
service dhcp 4-117
ip dhcp excluded-address 4-118
ip dhcp pool 4-118
network 4-119
default-router 4-120
domain-name 4-120

Downloaded from www.Manualslib.com manuals search engine

dns-server 4-121
next-server 4-121
bootfile 4-122
netbios-name-server 4-122
netbios-node-type 4-123
lease 4-124
host 4-124
client-identifier 4-125
hardware-address 4-126
clear ip dhcp binding 4-127
show ip dhcp binding 4-127
DNS Commands 4-128
ip host 4-128
clear host 4-129
ip domain-name 4-130
ip domain-list 4-130
ip name-server 4-131
ip domain-lookup 4-132
show hosts 4-133
show dns 4-133
show dns cache 4-134
clear dns cache 4-135
Interface Commands 4-136
interface 4-136
description 4-137
speed-duplex 4-137
negotiation 4-138
capabilities 4-139
flowcontrol 4-140
combo-forced-mode 4-141
shutdown 4-141
switchport broadcast packet-rate 4-142
clear counters 4-143
show interfaces status 4-144
show interfaces counters 4-145
show interfaces switchport 4-146
Mirror Port Commands 4-147

Downloaded from www.Manualslib.com manuals search engine

port monitor 4-147
show port monitor 4-148
Rate Limit Commands 4-149
rate-limit 4-149
Link Aggregation Commands 4-150
channel-group 4-151
lacp 4-151
lacp system-priority 4-153
lacp admin-key (Ethernet Interface) 4-153
lacp admin-key (Port Channel) 4-154
lacp port-priority 4-155
show lacp 4-156
Address Table Commands 4-159
mac-address-table static 4-159
clear mac-address-table dynamic 4-160
show mac-address-table 4-160
mac-address-table aging-time 4-161
show mac-address-table aging-time 4-162
Spanning Tree Commands 4-162
spanning-tree 4-163
spanning-tree mode 4-164
spanning-tree forward-time 4-165
spanning-tree hello-time 4-166
spanning-tree max-age 4-166
spanning-tree priority 4-167
spanning-tree pathcost method 4-167
spanning-tree transmission-limit 4-168
spanning-tree mst-configuration 4-168
mst vlan 4-169
mst priority 4-170
name 4-170
revision 4-171
max-hops 4-172
spanning-tree spanning-disabled 4-172
spanning-tree cost 4-173
spanning-tree port-priority 4-173
spanning-tree edge-port 4-174

Downloaded from www.Manualslib.com manuals search engine

spanning-tree portfast 4-175
spanning-tree link-type 4-176
spanning-tree mst cost 4-176
spanning-tree mst port-priority 4-177
spanning-tree protocol-migration 4-178
show spanning-tree 4-179
show spanning-tree mst configuration 4-180
VLAN Commands 4-181
Editing VLAN Groups 4-181
vlan database 4-181
vlan 4-182
Configuring VLAN Interfaces 4-183
interface vlan 4-183
switchport mode 4-184
switchport acceptable-frame-types 4-184
switchport ingress-filtering 4-185
switchport native vlan 4-186
switchport allowed vlan 4-187
switchport forbidden vlan 4-188
Displaying VLAN Information 4-188
show vlan 4-189
Configuring Protocol-based VLANs 4-189
protocol-vlan protocol-group (Configuring Groups) . . . 4-190
protocol-vlan protocol-group (Configuring Interfaces) . 4-191
show protocol-vlan protocol-group 4-191
show interfaces protocol-vlan protocol-group 4-192
Configuring Private VLANs 4-193
pvlan 4-193
show pvlan 4-193
GVRP and Bridge Extension Commands 4-194
bridge-ext gvrp 4-194
show bridge-ext 4-195
switchport gvrp 4-195
show gvrp configuration 4-196
garp timer 4-196
show garp timer 4-197
Priority Commands 4-198

Downloaded from www.Manualslib.com manuals search engine

Priority Commands (Layer 2) 4-198
switchport priority default 4-198
queue mode 4-199
queue bandwidth 4-200
queue cos-map 4-201
show queue mode 4-202
show queue bandwidth 4-202
show queue cos-map 4-203
Priority Commands (Layer 3 and 4) 4-204
map ip port (Global Configuration) 4-204
map ip port (Interface Configuration) 4-205
map ip precedence (Global Configuration) 4-205
map ip precedence (Interface Configuration) 4-206
map ip dscp (Global Configuration) 4-206
map ip dscp (Interface Configuration) 4-207
show map ip port 4-208
show map ip precedence 4-209
show map ip dscp 4-210
Multicast Filtering Commands 4-211
IGMP Snooping Commands 4-211
ip igmp snooping 4-211
ip igmp snooping vlan static 4-212
ip igmp snooping version 4-212
show ip igmp snooping 4-213
show mac-address-table multicast 4-213
IGMP Query Commands (Layer 2) 4-214
ip igmp snooping querier 4-214
ip igmp snooping query-count 4-215
ip igmp snooping query-interval 4-215
ip igmp snooping query-max-response-time 4-216
ip igmp snooping router-port-expire-time 4-217
Static Multicast Routing Commands 4-218
ip igmp snooping vlan mrouter 4-218
show ip igmp snooping mrouter 4-219
IGMP Commands (Layer 3) 4-220
ip igmp 4-220
ip igmp robustval 4-221

Downloaded from www.Manualslib.com manuals search engine

ip igmp query-interval 4-222
ip igmp max-resp-interval 4-222
ip igmp last-memb-query-interval 4-223
ip igmp version 4-224
show ip igmp interface 4-224
clear ip igmp group 4-225
show ip igmp groups 4-226
IP Interface Commands 4-227
Basic IP Configuration 4-227
ip address 4-227
ip default-gateway 4-229
show ip interface 4-229
show ip redirects 4-230
ping 4-230
Address Resolution Protocol (ARP) 4-232
arp 4-232
arp-timeout 4-233
clear arp-cache 4-233
show arp 4-233
ip proxy-arp 4-234
IP Routing Commands 4-235
Global Routing Configuration 4-235
ip routing 4-235
ip route 4-236
clear ip route 4-237
show ip route 4-237
show ip traffic 4-238
Routing Information Protocol (RIP) 4-239
router rip 4-240
timers basic 4-240
network 4-241
neighbor 4-242
version 4-242
ip rip receive version 4-243
ip rip send version 4-244
ip split-horizon 4-245
ip rip authentication key 4-246

Downloaded from www.Manualslib.com manuals search engine

ip rip authentication mode 4-246
show rip globals 4-247
show ip rip 4-248
Open Shortest Path First (OSPF) 4-249
router ospf 4-250
router-id 4-251
compatible rfc1583 4-251
default-information originate 4-252
timers spf 4-253
area range 4-254
area default-cost 4-254
summary-address 4-255
redistribute 4-256
network area 4-257
area stub 4-258
area nssa 4-259
area virtual-link 4-260
ip ospf authentication 4-262
ip ospf authentication-key 4-263
ip ospf message-digest-key 4-264
ip ospf cost 4-265
ip ospf dead-interval 4-265
ip ospf hello-interval 4-266
ip ospf priority 4-266
ip ospf retransmit-interval 4-267
ip ospf transmit-delay 4-268
show ip ospf 4-268
show ip ospf border-routers 4-269
show ip ospf database 4-270
show ip ospf interface 4-277
show ip ospf neighbor 4-278
show ip ospf summary-address 4-279
show ip ospf virtual-links 4-280
Multicast Routing Commands 4-280
Static Multicast Routing Commands 4-281
ip igmp snooping vlan mrouter 4-281
show ip igmp snooping mrouter 4-282

Downloaded from www.Manualslib.com manuals search engine

General Multicast Routing Commands 4-282
ip multicast-routing 4-282
show ip mroute 4-283
DVMRP Multicast Routing Commands 4-285
router dvmrp 4-285
probe-interval 4-286
nbr-timeout 4-287
report-interval 4-287
flash-update-interval 4-288
prune-lifetime 4-288
default-gateway 4-289
ip dvmrp 4-289
ip dvmrp metric 4-290
clear ip dvmrp route 4-291
show router dvmrp 4-291
show ip dvmrp route 4-292
show ip dvmrp neighbor 4-292
show ip dvmrp interface 4-293
PIM-DM Multicast Routing Commands 4-293
router pim 4-294
ip pim dense-mode 4-294
ip pim hello-interval 4-295
ip pim hello-holdtime 4-296
ip pim trigger-hello-interval 4-296
ip pim join-prune-holdtime 4-297
ip pim graft-retry-interval 4-298
ip pim max-graft-retries 4-298
show router pim 4-299
show ip pim interface 4-299
show ip pim neighbor 4-300
Router Redundancy Commands 4-300
Virtual Router Redundancy Protocol Commands 4-301
vrrp ip 4-301
vrrp authentication 4-302
vrrp priority 4-303
vrrp timers advertise 4-304
vrrp preempt 4-305

Downloaded from www.Manualslib.com manuals search engine

show vrrp 4-305
show vrrp interface 4-307
show vrrp router counters 4-308
show vrrp interface counters 4-308
clear vrrp router counters 4-309
clear vrrp interface counters 4-309
Hot Standby Router Protocol Commands 4-310
standby ip 4-310
standby priority 4-311
standby preempt 4-312
standby authentication 4-313
standby timers 4-314
standby track 4-315
show standby 4-316
show standby interface 4-318

Appendix A: Software Specifications A-1

Software Features A-1
Management Features A-2
Standards A-2
Management Information Bases A-3

Index

Appendix B: Troubleshooting Inde-1

Glossary

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 1
INTRODUCTION

The TigerSwitch 10/100/1000 provides a broad range of features for Layer 2 switching and Layer 3 routing. It includes a management agent that allows you to configure the features listed in this manual. The default configuration can be used for most of the features provided by this switch. However, there are many options that you should configure to maximize the switch's performance for your particular network environment.

Key Features

Feature	Description
Configuration Backup and Restore	Backup to TFTP server
Authentication	Console, Telnet, web – User name / password, RADIUS, TACACS+ Web – HTTPS; Telnet – SSH SNMP – Community strings, IP address filtering Port – IEEE 802.1x, MAC address filtering
Access Control Lists	Supports up to 32 IP or MAC ACLs
Access Control Lists	Supports up to 32 IP or MAC ACLs
DHCP Client, Relay and Server	Supported
DNS Server	Supported
Port Configuration	Speed, duplex mode and flow control

Downloaded from www.Manualslib.com manuals search engine

Feature	Description
Rate Limiting	Input and output rate limiting per port
Port Mirroring	One or more ports mirrored to single analysis port
Port Trunking	Supports up to 6 trunks using either static or dynamic trunking (LACP)
Broadcast Storm Control	Supported
Address Table	Up to 16K MAC addresses in the forwarding table, 1024 static MAC addresses; Up to 4K IP address entries in the ARP cache, 128 static IP routes
IEEE 802.1D Bridge	Supports dynamic data switching and addresses learning
Store-and-Forward Switching	Supported to ensure wire-speed switching while eliminating bad frames
Spanning Tree Protocol	Supports standard STP, Rapid Spanning Tree Protocol (RSTP), and Multiple Spanning Trees (MSTP)
Virtual LANs	Up to 255 using IEEE 802.1Q, port-based, protocol-based, or private VLANs
Traffic Prioritization	Default port priority, traffic class map, queue scheduling, IP Precedence, or Differentiated Services Code Point (DSCP)
Router Redundancy	Router backup is provided with the Virtual Router Redundancy Protocol (VRRP) and the Hot Standby Router Protocol (HSRP)
IP Routing	Routing Information Protocol (RIP), Open Shortest Path First (OSPF), static routes
ARP	Static and dynamic address configuration, proxy ARP
Multicast Filtering	Supports IGMP snooping and query for Layer 2, and IGMP for Layer 3
Multicast Routing	Supports DVMRP and PIM-DM

Downloaded from www.Manualslib.com manuals search engine

Description of Software Features

The switch provides a wide range of advanced performance enhancing features. Flow control eliminates the loss of packets due to bottlenecks caused by port saturation. Broadcast storm suppression prevents broadcast traffic storms from engulfing the network. Port-based and protocol-based VLANs, plus support for automatic GVRP VLAN registration provide traffic security and efficient use of network bandwidth. CoS priority queueing ensures the minimum delay for moving real-time multimedia data across the network. While multicast filtering and routing provides support for real-time network applications. Some of the management features are briefly described below.

Configuration Backup and Restore – You can save the current configuration settings to a file on a TFTP server, and later download this file to restore the switch configuration settings.

Authentication – This switch authenticates management access via the console port, Telnet or web browser. User names and passwords can be configured locally or can be verified via a remote authentication server (i.e., RADIUS or TACACS+). Port-based authentication is also supported via the IEEE 802.1x protocol. This protocol uses Extensible Authentication Protocol over LANs (EAPOL) to request a user name and password from the 802.1x client, and then uses the EAP between the switch and the authentication server to verify the client's right to access the network via an authentication server.

Other authentication options include HTTPS for secure management access via the web, SSH for secure management access over a Telnet-equivalent connection, IP address filtering for SNMP/web/Telnet management access, and MAC address filtering for port access.

Access Control Lists – ACLs provide packet filtering for IP frames (based on address, protocol, TCP/UDP port number or TCP control code) or any frames (based on MAC address or Ethernet type). ACLs can

Downloaded from www.Manualslib.com manuals search engine

by used to improve performance by blocking unnecessary network traffic or to implement security controls by restricting access to specific network resources or protocols.

DHCP Server and DHCP Relay – A DHCP server is provided to assign IP addresses to host devices. Since DHCP uses a broadcast mechanism, a DHCP server and its client must physically reside on the same subnet. Since it is not practical to have a DHCP server on every subnet, DHCP Relay is also supported to allow dynamic configuration of local clients from a DHCP server located in a different network.

Port Configuration – You can manually configure the speed, duplex mode, and flow control used on specific ports, or use auto-negotiation to detect the connection settings used by the attached device. Use the full-duplex mode on ports whenever possible to double the throughput of switch connections. Flow control should also be enabled to control network traffic during periods of congestion and prevent the loss of packets when port buffer thresholds are exceeded. The switch supports flow control based on the IEEE 802.3x standard.

Rate Limiting – This feature controls the maximum rate for traffic transmitted or received on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic into or out of the network. Traffic that falls within the rate limit is transmitted, while packets that exceed the acceptable amount of traffic are dropped.

Port Mirroring – The switch can unobtrusively mirror traffic from any port to a monitor port. You can then attach a protocol analyzer or RMON probe to this port to perform traffic analysis and verify connection integrity.

Port Trunking – Ports can be combined into an aggregate connection. Trunks can be manually set up or dynamically configured using IEEE 802.3ad Link Aggregation Control Protocol (LACP). The additional ports dramatically increase the throughput across any connection, and provide

Downloaded from www.Manualslib.com manuals search engine

redundancy by taking over the load if a port in the trunk should fail. The switch supports up to 6 trunks.

Broadcast Storm Control – Broadcast suppression prevents broadcast traffic from overwhelming the network. When enabled on a port, the level of broadcast traffic passing through the port is restricted. If broadcast traffic rises above a pre-defined threshold, it will be throttled until the level falls back beneath the threshold.

Static Addresses – A static address can be assigned to a specific interface on this switch. Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table. Static addresses can be used to provide network security by restricting access for a known host to a specific port.

IEEE 802.1D Bridge – The switch supports IEEE 802.1D transparent bridging. The address table facilitates data switching by learning addresses, and then filtering or forwarding traffic based on this information. The address table supports up to 16K addresses.

Store-and-Forward Switching – The switch copies each frame into its memory before forwarding them to another port. This ensures that all frames are a standard Ethernet size and have been verified for accuracy with the cyclic redundancy check (CRC). This prevents bad frames from entering the network and wasting bandwidth.

To avoid dropping frames on congested ports, the switch provides 1 MB for frame buffering. This buffer can queue packets awaiting transmission on congested networks.

Spanning Tree Protocol – The switch supports these spanning tree protocols:

Spanning Tree Protocol (STP, IEEE 802.1D) – This protocol adds a level of fault tolerance by allowing two or more redundant connections to be created between a pair of LAN segments. When there are multiple physical

Downloaded from www.Manualslib.com manuals search engine

paths between segments, this protocol will choose a single path and disable all others to ensure that only one route exists between any two stations on the network. This prevents the creation of network loops. However, if the chosen path should fail for any reason, an alternate path will be activated to maintain the connection.

Rapid Spanning Tree Protocol (RSTP, IEEE 802.1w) – This protocol reduces the convergence time for network topology changes to about 10% of that required by the older IEEE 802.1D STP standard. It is intended as a complete replacement for STP, but can still interoperate with switches running the older standard by automatically reconfiguring ports to STP-compliant mode if they detect STP protocol messages from attached devices.

Multiple Spanning Tree Protocol (MSTP, IEEE 802.1s) – This protocol is a direct extension of RSTP. It can provide an independent spanning tree for different VLANs. It simplifies network management, provides for even faster convergence than RSTP by limiting the size of each region, and prevents VLAN members from being segmented from the rest of the group (as sometimes occurs with IEEE 802.1D STP).

Virtual LANs – The switch supports up to 255 VLANs. A Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. The switch supports tagged VLANs based on the IEEE 802.1Q standard. Members of VLAN groups can be dynamically learned via GVRP, or ports can be manually assigned to a specific set of VLANs. This allows the switch to restrict traffic to the VLAN groups to which a user has been assigned. By segmenting your network into VLANs, you can:

- Eliminate broadcast storms which severely degrade performance in a flat network.
- Simplify network management for node changes/moves by remotely configuring VLAN membership for any port, rather than having to manually change the network connection.
- Provide data security by restricting all traffic to the originating VLAN,

Downloaded from www.Manualslib.com manuals search engine

except where a connection is explicitly defined via the switch's routing service.

- Use private VLANs to restrict traffic to pass only between data ports and the uplink ports, thereby isolating adjacent ports within the same VLAN, and allowing you to limit the total number of VLANs that need to be configured.

Traffic Prioritization – This switch prioritizes each packet based on the required level of service, using four priority queues with strict or Weighted Round Robin Queuing. It uses IEEE 802.1p and 802.1Q tags to prioritize incoming traffic based on input from the end-station application. These functions can be used to provide independent priorities for delay-sensitive data and best-effort data.

This switch also supports several common methods of prioritizing layer 3/4 traffic to meet application requirements. Traffic can be prioritized based on the priority bits in the IP frame's Type of Service (ToS) octet. When these services are enabled, the priorities are mapped to a Class of Service value by the switch, and the traffic then sent to the corresponding output queue.

IP Routing – The switch provides Layer 3 IP routing. To maintain a high rate of throughput, the switch forwards all traffic passing within the same segment, and routes only traffic that passes between different subnetworks. The wire-speed routing provided by this switch lets you easily link network segments or VLANs together without having to deal with the bottlenecks or configuration hassles normally associated with conventional routers.

Routing for unicast traffic is supported with the Routing Information Protocol (RIP) and the Open Shortest Path First (OSPF) protocol.

RIP – This protocol uses a distance-vector approach to routing. Routes are determined on the basis of minimizing the distance vector, or hop count, which serves as a rough estimate of transmission cost.

Downloaded from www.Manualslib.com manuals search engine

OSPF – This approach uses a link state routing protocol to generate a shortest-path tree, then builds up its routing table based on this tree. OSPF produces a more stable network because the participating routers act on network changes predictably and simultaneously, converging on the best route more quickly than RIP.

Router Redundancy – Hot Standby Router Protocol (HSRP) and Virtual Router Redundancy Protocol (VRRP) both use a virtual IP address to support a primary router and multiple backup routers. The backups can be configured to take over the workload if the master fails or to load share the traffic. The primary goal of these protocols is to allow a host device which has been configured with a fixed gateway to maintain network connectivity in case the primary gateway goes down.

Address Resolution Protocol – The switch uses ARP and Proxy ARP to convert between IP addresses and MAC (i.e., hardware) addresses. This switch supports conventional ARP, which locates the MAC address corresponding to a given IP address. This allows the switch to use IP addresses for routing decisions and the corresponding MAC addresses to forward packets from one hop to the next. You can configure either static or dynamic entries in the ARP cache.

Proxy ARP allows hosts that do not support routing to determine the MAC address of a device on another network or subnet. When a host sends an ARP request for a remote network, the switch checks to see if it has the best route. If it does, it sends its own MAC address to the host. The host then sends traffic for the remote destination via the switch, which uses its own routing table to reach the destination on the other network.

Multicast Filtering – Specific multicast traffic can be assigned to its own VLAN to ensure that it does not interfere with normal network traffic and to guarantee real-time delivery by setting the required priority level for the designated VLAN. The switch uses IGMP Snooping and Query at Layer 2 and IGMP at Layer 3 to manage multicast group registration.

Downloaded from www.Manualslib.com manuals search engine

Multicast Routing – Routing for multicast packets is supported by the Distance Vector Multicast Routing Protocol (DVMRP) and Protocol-Independent Multicasting - Dense Mode (PIM-DM). These protocols work in conjunction with IGMP to filter and route multicast traffic. DVMRP is a more comprehensive implementation that maintains its own routing table, but is gradually being replacing by most network managers with PIM, Dense Mode and Sparse Mode. PIM is a very simple protocol that uses the routing table of the unicast routing protocol enabled on an interface. Dense Mode is designed for areas where the probability of multicast clients is relatively high, and the overhead of frequent flooding is justified. While Sparse mode is designed for network areas, such as the Wide Area Network, where the probability of multicast clients is low. This switch currently supports DVMRP and PIM-DM.

Downloaded from www.Manualslib.com manuals search engine

System Defaults

The switch's system defaults are provided in the configuration file "Factory_Default_Config.cfg." To reset the switch defaults, this file should be set as the startup configuration file (page 3-27).

The following table lists some of the basic system defaults.

Function	Parameter	Default
Console Port Connection	Baud Rate	auto
	Data bits	8
	Stop bits	1
	Parity	none
	Local Console Timeout	0 (disabled)
Authentication	Privileged Exec Level	Username "admin" Password "admin"
	Normal Exec Level	Username "guest" Password "guest"
	Enable Privileged Exec from Normal Exec Level	Password "super"
	RADIUS Authentication	Disabled
	TACACS Authentication	Disabled
	802.1x Port Authentication	Disabled
	HTTPS	Enabled
	SSH	Enabled
	Port Security	Disabled
Web Management	HTTP Server	Enabled
	HTTP Port Number	80
	HTTP Secure Server	Enabled
	HTTP Secure Port Number	443

Downloaded from www.Manualslib.com manuals search engine

Function	Parameter	Default
SNMP	Community Strings	"public" (read only) "private" (read/write)
	Traps	Authentication traps: enabled Link-up-down events: enabled
	IP Filtering	Disabled
Port Configuration	Admin Status	Enabled
	Auto-negotiation	Enabled
	Flow Control	Disabled
	Port Capability	1000BASE-T – 10 Mbps half duplex 10 Mbps full duplex 100 Mbps half duplex 100 Mbps full duplex 1000 Mbps full duplex Full-duplex flow control disabled Symmetric flow control disabled 1000BASE-SX/LX/LH – 1000 Mbps full duplex Full-duplex flow control disabled Symmetric flow control disabled
Rate Limiting	Input and output limits	Disabled
Port Trunking	Static Trunks	None
	LACP	Disabled
Broadcast Storm Protection	Status	Enabled (all ports)
	Broadcast Limit Rate	500 packets per second
Spanning Tree Protocol	Status	Enabled, MSTP (Defaults: All values based on IEEE 802.1s)
	Fast Forwarding (Edge Port)	Disabled
Address Table	Aging Time	300 seconds

Downloaded from www.Manualslib.com manuals search engine

Function	Parameter	Default
Virtual LANs	Default VLAN	1
	PVID	1
	Acceptable Frame Type	All
	Ingress Filtering	Disabled
	Switchport Mode (Egress Mode)	Hybrid: tagged/untagged frames
	GVRP (global)	Disabled
	GVRP (port interface)	Disabled
Traffic Prioritization	Ingress Port Priority	0
	Weighted Round Robin	Queue: 0 1 2 3 4 5 6 7 Priority: 2 0 1 3 4 5 6 7
	IP Precedence Priority	Disabled
	IP DSCP Priority	Disabled
IP Settings	Management. VLAN	Any VLAN configured with an IP address
IP Settings	IP Address	0.0.0.0
	Subnet Mask	255.0.0.0
	Default Gateway	0.0.0.0
	DHCP	Client: Disabled Relay: Disabled Server: Disabled
	DNS	Server: Disabled
	BOOTP	Disabled
	ARP	Enabled Cache Timeout: 20 minutes Proxy: Disabled
Unicast Routing	RIP	Disabled
	OSPF	Disabled

Downloaded from www.Manualslib.com manuals search engine

Function	Parameter	Default
Router Redundancy	HSRP	Disabled
	VRRP	Disabled
Multicast Filtering	IGMP Snooping (Layer 2)	Snooping: Enabled Querier: Disabled
	IGMP (Layer 3)	Disabled
Multicast Routing	DVMRP	Disabled
	PIM-DM	Disabled
System Log	Status	Enabled
	Messages Logged	Levels 0-7 (all)
	Messages Logged to Flash	Levels 0-3
SMTP Email Alerts	Event Handler	Disabled
SNTP	Clock Synchronization	Disabled

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 2
INITIAL CONFIGURATION

Connecting to the Switch

Configuration Options

The switch includes a built-in network management agent. The agent offers a variety of management options, including SNMP, RMON and a web-based interface. A PC may also be connected directly to the switch for configuration and monitoring via a command line interface (CLI).

Note: The IP address for this switch is unassigned by default. To change this address, see "Setting an IP Address" on page 2-7.

The switch's HTTP web agent allows you to configure switch parameters, monitor port connections, and display statistics using a standard web browser such as Netscape Navigator version 6.2 and higher or Microsoft IE version 5.0 and higher. The switch's web management interface can be accessed from any computer attached to the network.

The CLI program can be accessed by a direct connection to the RS-232 serial console port on the switch, or remotely by a Telnet connection over the network.

The switch's management agent also supports SNMP (Simple Network Management Protocol). This SNMP agent permits the switch to be managed from any system in the network using network management software such as HP OpenView.

Downloaded from www.Manualslib.com manuals search engine

The switch's web interface, CLI configuration program, and SNMP agent allow you to perform the following management functions:

- Set user names and passwords for up to 16 users
- Set an IP interface for any VLAN
- Configure SNMP parameters
- Enable/disable any port
- Set the speed/duplex mode for any port
- Configure the bandwidth of any port by limiting input or output rates
- Configure up to 255 IEEE 802.1Q VLANs
- Enable GVRP automatic VLAN registration
- Configure IP routing for unicast or multicast traffic
- Configure router redundancy
- Configure IGMP multicast filtering
- Upload and download system firmware via TFTP
- Upload and download switch configuration files via TFTP
- Configure Spanning Tree parameters
- Configure Class of Service (CoS) priority queuing
- Configure up to 6 static or LACP trunks
- Enable port mirroring
- Set broadcast storm control on any port
- Display system information and statistics

Downloaded from www.Manualslib.com manuals search engine

Required Connections

The switch provides an RS-232 serial port that enables a connection to a PC or terminal for monitoring and configuring the switch. A null-modem console cable is provided with the switch.

Attach a VT100-compatible terminal, or a PC running a terminal emulation program to the switch. You can use the console cable provided with this package, or use a null-modem cable that complies with the wiring assignments shown in the Installation Guide.

To connect a terminal to the console port, complete the following steps:

1. Connect the console cable to the serial port on a terminal, or a PC running terminal emulation software, and tighten the captive retaining screws on the DB-9 connector.

2. Connect the other end of the cable to the RS-232 serial port on the switch.

3. Make sure the terminal emulation software is set as follows:
   - Select the appropriate serial port (COM port 1 or COM port 2).
   - Set to any of the following baud rates: 9600, 19200, 38400, 57600, 115200
     (Note: Set to 9600 baud if want to view all the system initialization messages.)
   - Set the data format to 8 data bits, 1 stop bit, and no parity.
   - Set flow control to none.
   - Set the emulation mode to VT100.
   - When using HyperTerminal, select Terminal keys, not Windows keys.

Notes: 1. When using HyperTerminal with Microsoft® Windows® 2000, make sure that you have Windows 2000 Service Pack 2 or later installed. Windows 2000 Service Pack 2 fixes the problem of arrow keys not functioning in HyperTerminal's VT100 emulation. See www.microsoft.com for information on

Downloaded from www.Manualslib.com manuals search engine

Windows 2000 service packs.

2. Refer to "Line Commands" on page 4-15 for a complete description of console configuration options.

3. Once you have set up the terminal correctly, the console login screen will be displayed.

For a description of how to use the CLI, see "Using the Command Line Interface" on page 4-1. For a list of all the CLI commands and detailed information on using the CLI, refer to "Command Groups" on page 4-13.

Downloaded from www.Manualslib.com manuals search engine

Remote Connections

Prior to accessing the switch's onboard agent via a network connection, you must first configure it with a valid IP address, subnet mask, and default gateway using a console connection, DHCP or BOOTP protocol.

The IP address for this switch is unassigned by default. To manually configure this address or enable dynamic address assignment via DHCP or BOOTP, see "Setting an IP Address" on page 2-7.

Notes: **1.** This switch supports four concurrent Telnet/SSH sessions.

2. Each VLAN group can be assigned its own IP interface address (page 2-7). You can manage the switch via any of these addresses.

After configuring the switch's IP parameters, you can access the onboard configuration program from anywhere within the attached network. The onboard configuration program can be accessed using Telnet from any computer attached to the network. The switch can also be managed by any computer using a web browser (Internet Explorer 5.0 or above, or Netscape Navigator 6.2 or above), or from a network computer using SNMP network management software.

Note: The onboard program only provides access to basic configuration functions. To access the full range of SNMP management functions, you must use SNMP-based network management software.

Basic Configuration

Console Connection

The CLI program provides two different command levels — normal access level (Normal Exec) and privileged access level (Privileged Exec). The commands available at the Normal Exec level are a limited subset of

Downloaded from www.Manualslib.com manuals search engine

those available at the Privileged Exec level and allow you to only display information and use basic utilities. To fully configure the switch parameters, you must access the CLI at the Privileged Exec level.

Access to both CLI levels are controlled by user names and passwords. The switch has a default user name and password for each level. To log into the CLI at the Privileged Exec level using the default user name and password, perform these steps:

1. To initiate your console connection, press <Enter>. The "User Access Verification" procedure starts.
2. At the Username prompt, enter "admin."
3. At the Password prompt, also enter "admin." (The password characters are not displayed on the console screen.)
4. The session is opened and the CLI displays the "Console#" prompt indicating you have access at the Privileged Exec level.

Setting Passwords

Note: If this is your first time to log into the CLI program, you should define new passwords for both default user names using the "username" command, record them and put them in a safe place.

Passwords can consist of up to 8 alphanumeric characters and are case sensitive. To prevent unauthorized access to the switch, set the passwords as follows:

1. Open the console interface with the default user name and password "admin" to access the Privileged Exec level.
2. Type "configure" and press <Enter>.
3. Type "username guest password 0 *password*," for the Normal Exec level, where *password* is your new password. Press <Enter>.

Downloaded from www.Manualslib.com manuals search engine

4. Type "username admin password 0 *password*," for the Privileged Exec level, where *password* is your new password. Press <Enter>.

```
Username: admin
Password:

    CLI session with theCLI session with the SMC8612XL3 is opened.
To end the CLI session, enter [Exit].

Console#configure
Console(config)#username guest password 0 [password]
Console(config)#username admin password 0 [password]
Console(config)#
```

Setting an IP Address

You must establish IP address information for the switch to obtain management access through the network. This can be done in either of the following ways:

Manual — You have to input the information, including IP address and subnet mask. If your management station is not in the same IP subnet as the switch, you will also need to specify the default gateway router.

Dynamic — The switch sends IP configuration requests to BOOTP or DHCP address allocation servers on the network.

Manual Configuration

You can manually assign an IP address to the switch. You may also need to specify a default gateway that resides between this device and management stations that exist on another network segment (if routing is not enabled on this switch). Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. Anything outside this format will not be accepted by the CLI program.

Note: The IP address for this switch is unassigned by default.

Before you can assign an IP address to the switch, you must obtain the following information from your network administrator:

Downloaded from www.Manualslib.com manuals search engine

- IP address for the switch
- Default gateway for the network
- Network mask for this network

To assign an IP address to the switch, complete the following steps:

1. From the Privileged Exec level global configuration mode prompt, type "interface vlan 1" to access the interface-configuration mode. Press <Enter>.
2. Type "ip address *ip-address netmask*," where "ip-address" is the switch IP address and "netmask" is the network mask for the network. Press <Enter>.
3. Type "exit" to return to the global configuration mode prompt. Press <Enter>.
4. To set the IP address of the default gateway for the network to which the switch belongs, type "ip default-gateway *gateway*," where "gateway" is the IP address of the default gateway. Press <Enter>.

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.5 255.255.255.0
Console(config-if)#exit
Console(config)#ip default-gateway 192.168.1.254
Console(config)#
```

Dynamic Configuration

If you select the "bootp" or "dhcp" option, IP will be enabled but will not function until a BOOTP or DHCP reply has been received. You therefore need to use the "ip dhcp restart client" command to start broadcasting service requests. Requests will be sent periodically in an effort to obtain IP configuration information. (BOOTP and DHCP values can include the IP address, subnet mask, and default gateway.)

Downloaded from www.Manualslib.com manuals search engine

If the "bootp" or "dhcp" option is saved to the startup-config file (step 6), then the switch will start broadcasting service requests as soon as it is powered on.

To automatically configure the switch by communicating with BOOTP or DHCP address allocation servers on the network, complete the following steps:

1. From the Global Configuration mode prompt, type "interface vlan 1" to access the interface-configuration mode. Press <Enter>.

2. At the interface-configuration mode prompt, use one of the following commands:

    - To obtain IP settings via DHCP, type "ip address dhcp" and press <Enter>.
    - To obtain IP settings via BOOTP, type "ip address bootp" and press <Enter>.

3. Type "end" to return to the Privileged Exec mode. Press <Enter>.

4. Type "ip dhcp restart client" to begin broadcasting service requests. Press <Enter>.

5. Wait a few minutes, and then check the IP configuration settings by typing the "show ip interface" command. Press <Enter>.

Downloaded from www.Manualslib.com manuals search engine

6. Then save your configuration changes by typing "copy running-config startup-config." Enter the startup file name and press <Enter>.

```
Console(config)#interface vlan 1
Console(config-if)#ip address dhcp
Console(config-if)#end
Console#ip dhcp restart client
Console#show ip interface
 IP address and netmask: 192.168.1.54 255.255.255.0 on VLAN 1,
 and address mode: User specified.
Console#copy running-config startup-config
Startup configuration file name []: startup
\Write to FLASH Programming.

\Write to FLASH finish.
Success.
```

Enabling SNMP Management Access

The switch can be configured to accept management commands from Simple Network Management Protocol (SNMP) applications such as HP OpenView. You can configure the switch to (1) respond to SNMP requests or (2) generate SNMP traps.

When SNMP management stations send requests to the switch (either to return information or to set a parameter), the switch provides the requested data or sets the specified parameter. The switch can also be configured to send information to SNMP managers (without being requested by the managers) through trap messages, which inform the manager that certain events have occurred.

Community Strings

Community strings are used to control management access to SNMP stations, as well as to authorize SNMP stations to receive trap messages from the switch. You therefore need to assign community strings to specified users or user groups, and set the access level.

Downloaded from www.Manualslib.com manuals search engine

The default strings are:

- **public** - with read-only access. Authorized management stations are only able to retrieve MIB objects.
- **private** - with read-write access. Authorized management stations are able to both retrieve and modify MIB objects.

Note: If you do not intend to utilize SNMP, we recommend that you delete both of the default community strings. If there are no community strings, then SNMP management access to the switch is disabled.

To prevent unauthorized access to the switch via SNMP, it is recommended that you change the default community strings.

To configure a community string, complete the following steps:

1. From the Privileged Exec level global configuration mode prompt, type "snmp-server community *string mode*," where "string" is the community access string and "mode" is **rw** (read/write) or **ro** (read only). Press <Enter>. (Note that the default mode is read only.)
2. To remove an existing string, simply type "no snmp-server community *string*," where "string" is the community access string to remove. Press <Enter>.

```
Console(config)#snmp-server community admin rw
Console(config)#snmp-server community private
Console(config)#
```

Trap Receivers

You can also specify SNMP stations that are to receive traps from the switch.

To configure a trap receiver, complete the following steps:

Downloaded from www.Manualslib.com manuals search engine

1. From the Privileged Exec level global configuration mode prompt, type "snmp-server host *host-address community-string*," where "host-address" is the IP address for the trap receiver and "community-string" is the string associated with that host. Press <Enter>.

2. In order to configure the switch to send SNMP notifications, you must enter at least one snmp-server enable traps command. Type "snmp-server enable traps *type*," where "type" is either **authentication** or **link-up-down**. Press <Enter>.

```
Console(config)#snmp-server enable traps link-up-down
Console(config)#
```

Saving Configuration Settings

Configuration commands only modify the running configuration file and are not saved when the switch is rebooted. To save all your configuration changes in nonvolatile storage, you must copy the running configuration file to the start-up configuration file using the "copy" command.

To save the current configuration settings, enter the following command:

1. From the Privileged Exec mode prompt, type "copy running-config startup-config" and press <Enter>.

2. Enter the name of the start-up file. Press <Enter>.

```
Console#copy running-config startup-config
Startup configuration file name []: startup
\Write to FLASH Programming.

\Write to FLASH finish.
Success.

Console#
```


Downloaded from www.Manualslib.com manuals search engine

Managing System Files

The switch's flash memory supports three types of system files that can be managed by the CLI program, web interface, or SNMP. The switch's file system allows files to be uploaded and downloaded, copied, deleted, and set as a start-up file.

The three types of files are:

- **Configuration** — This file stores system configuration information and is created when configuration settings are saved. Saved configuration files can be selected as a system start-up file or can be uploaded via TFTP to a server for backup. A file named "Factory_Default_Config.cfg" contains all the system default settings and cannot be deleted from the system. See "Saving or Restoring Configuration Settings" on page 3-26 for more information.

- **Operation Code** — System software that is executed after boot-up, also known as run-time code. This code runs the switch operations and provides the CLI and web management interfaces. See "Managing Firmware" on page 3-24 for more information.

- **Diagnostic Code** — Software that is run during system boot-up, also known as POST (Power On Self-Test).

Due to the size limit of the flash memory, the switch supports only two operation code files. However, you can have as many diagnostic code files and configuration files as available flash memory space allows.

In the system flash memory, one file of each type must be set as the start-up file. During a system boot, the diagnostic and operation code files set as the start-up file are run, and then the start-up configuration file is loaded.

Downloaded from www.Manualslib.com manuals search engine

Note that configuration files should be downloaded using a file name that reflects the contents or usage of the file settings. If you download directly to the running-config, the system will reboot, and the settings will have to be copied from the running-config to a permanent file.

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 3
CONFIGURING THE SWITCH

Using the Web Interface

This switch provides an embedded HTTP web agent. Using a web browser you can configure the switch and view statistics to monitor network activity. The web agent can be accessed by any computer on the network using a standard web browser (Internet Explorer 5.0 or above, or Netscape Navigator 6.2 or above).

Note: You can also use the Command Line Interface (CLI) to manage the switch over a serial connection to the console port or via Telnet. For more information on using the CLI, refer to Chapter 4 "Command Line Interface."

Prior to accessing the switch from a web browser, be sure you have first performed the following tasks:

1. Configure the switch with a valid IP address, subnet mask, and default gateway using an out-of-band serial connection, BOOTP or DHCP protocol. (See "Setting an IP Address" on page 2-7.)

2. Set user names and passwords using an out-of-band serial connection. Access to the web agent is controlled by the same user names and passwords as the onboard configuration program. (See "Setting Passwords" on page 2-6.)

3. After you enter a user name and password, you will have access to the system configuration program.

Notes: 1. You are allowed three attempts to enter the correct password;

Downloaded from www.Manualslib.com manuals search engine

on the third failed attempt the current connection is terminated.

2. If you log into the web interface as guest (Normal Exec level), you can view the configuration settings or change the guest password. If you log in as "admin" (Privileged Exec level), you can change the settings on any page.

3. If the path between your management station and this switch does not pass through any device that uses the Spanning Tree Algorithm, then you can set the switch port attached to your management station to fast forwarding (i.e., enable Admin Edge Port) to improve the switch's response time to management commands issued through the web interface. See "Configuring Interface Settings" on page 3-140.

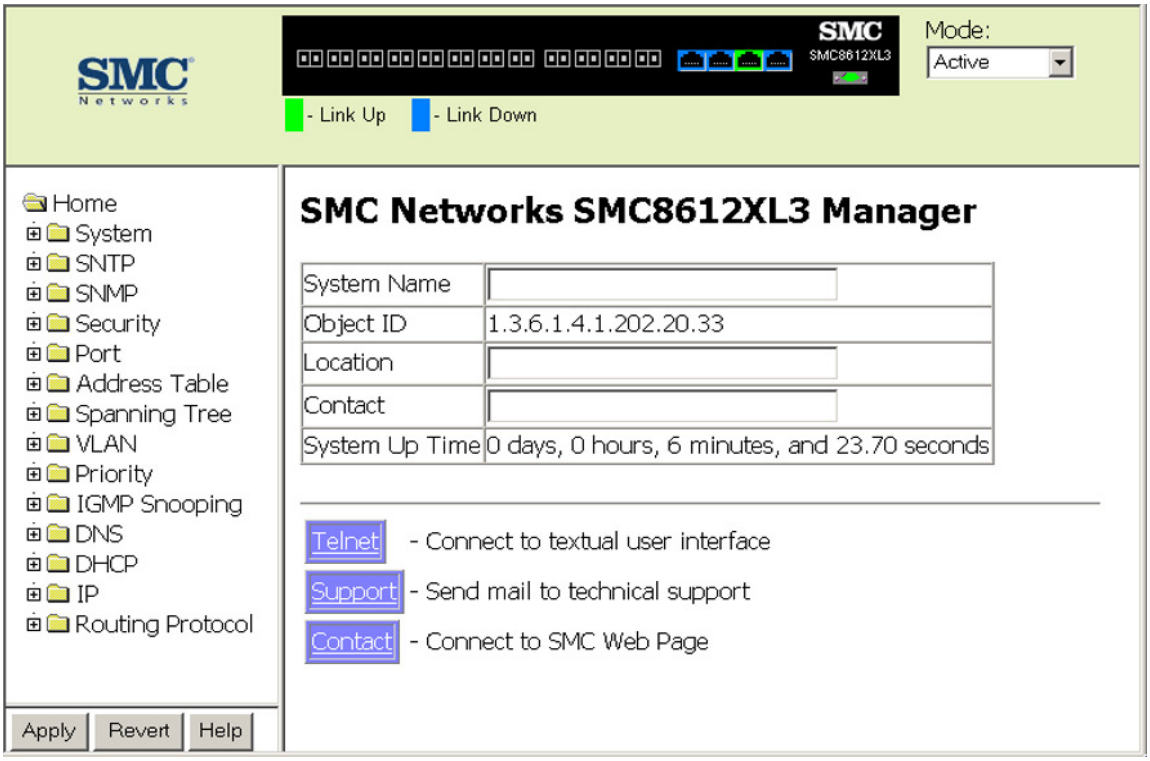
Downloaded from www.Manualslib.com manuals search engine

Navigating the Web Browser Interface

To access the web-browser interface you must first enter a user name and password. The administrator has Read/Write access to all configuration parameters and statistics. The default user name and password for the administrator is "admin."

Home Page

When your web browser connects with the switch's web agent, the home page is displayed as shown below. The home page displays the Main Menu on the left side of the screen and System Information on the right side. The Main Menu links are used to navigate to other menus, and display configuration parameters and statistics.



Configuration Options

Configurable parameters have a dialog box or a drop-down list. Once a configuration change has been made on a page, be sure to click on the

Downloaded from www.Manualslib.com manuals search engine

"Apply" or "Apply Changes" button to confirm the new setting. The following table summarizes the web page configuration buttons.

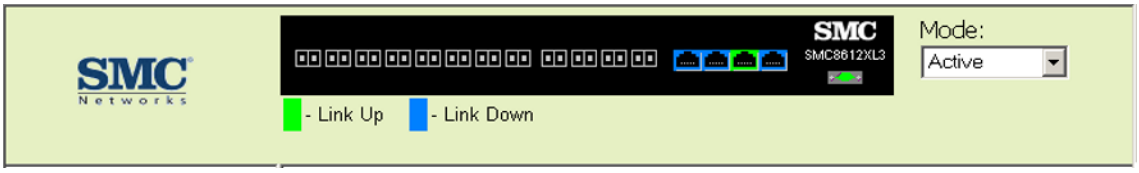
Button	Action
Revert	Cancels specified values and restores current values prior to pressing "Apply" or "Apply Changes."
Refresh	Immediately updates values for the current page.
Apply	Sets specified values to the system.
Apply Changes	Sets specified values to the system.

Notes: **1.** To ensure proper screen refresh, be sure that Internet Explorer 5.x is configured as follows: Under the menu "Tools / Internet Options / General / Temporary Internet Files / Settings," the setting for item "Check for newer versions of stored pages" should be "Every visit to the page."

2. When using Internet Explorer 5.0, you may have to manually refresh the screen after making configuration changes by pressing the browser's refresh button.

Panel Display

The web agent displays an image of the switch's ports. The Mode can be set to display different information for the ports, including Active (i.e., up or down), Duplex (i.e., half or full duplex), or Flow Control (i.e., with or without flow control). Clicking on the image of a port opens the Port Configuration page as described on page 3-93.



Main Menu

Using the onboard web agent, you can define system parameters, manage and control the switch, and all its ports, or monitor network conditions.

Downloaded from www.Manualslib.com manuals search engine

The following table briefly describes the selections available from this program.

Menu	Description	Page
System		3-14
System Information	Provides basic system description, including contact information	3-14
Switch Information	Shows the number of ports, hardware/firmware version numbers, and power status	3-16
Bridge Extension	Shows the bridge extension parameters	3-18
Firmware	Manages code image files	3-24
Configuration	Manages switch configuration files	3-26
Log		3-28
Logs	Sends error messages to a logging process	3-28
System Logs	Stores and displays error messages	3-32
Remote Logs	Configures the logging of messages to a remote logging process	3-30
Reset	Restarts the switch	3-33
SNTP		3-33
Configuration	Configures SNTP client settings, including broadcast mode or a specified list of servers	3-34
Clock Time Zone	Sets the local time zone for the system clock	3-35
SNMP		3-36
Configuration	Configures community strings and related trap functions	3-37
IP Filtering	Sets IP addresses of clients allowed management access	3-41
Security		3-42
Passwords	Assigns a new password for the current user	3-43
Authentication Settings	Configures authentication sequence, RADIUS and TACACS	3-44
HTTPS Settings	Configures secure HTTP settings	3-48

Downloaded from www.Manualslib.com manuals search engine

Menu	Description	Page
SSH		3-50
Settings	Configures Secure Shell server settings	3-55
Host-Key Settings	Generates the host key pair (public and private)	3-53
Port Security	Configures per port security, including status, response for security breach, and maximum allowed MAC addresses	3-56
802.1x	Port authentication	3-60
Information	Displays global configuration settings	3-61
Configuration	Configures protocol parameters	3-64
Port Configuration	Sets the authentication mode for individual ports	3-65
Statistics	Displays protocol statistics for the selected port	3-67
ACL		3-72
Configuration	Configures packet filtering based on IP or MAC addresses	3-72
Mask Configuration	Controls the order in which ACL rules are checked	3-81
Port Binding	Binds a port to the specified ACL	3-87
IP Filter	Configures IP addresses that are allowed management access	3-69
Port		3-89
Port Information	Displays port connection status	3-89
Trunk Information	Displays trunk connection status	3-89
Port Configuration	Configures port connection settings	3-93
Trunk Configuration	Configures trunk connection settings	3-93
Trunk Membership	Specifies ports to group into static trunks	3-97
LACP		3-96
Configuration	Allows ports to dynamically join trunks	3-99
Aggregation Port	Configures parameters for link aggregation group members	3-101
Port Counters	Displays statistics for LACP protocol messages	3-104

Downloaded from www.Manualslib.com manuals search engine

Menu	Description	Page
Port Internal Information	Displays settings and operational state for the local side	3-106
Port Neighbors Information	Displays settings and operational state for the remote side	3-108
Port Broadcast Control	Sets the broadcast storm threshold for each port	3-111
Mirror Port Configuration	Sets the source and target ports for mirroring	3-113
Rate Limit		3-115
Input Port Configuration	Sets the input rate limit for each port	3-115
Input Trunk Configuration	Sets the input rate limit for each trunk	3-115
Output Port Configuration	Sets the output rate limit for each port	3-115
Output Trunk Configuration	Sets the output rate limit for each trunk	3-115
Port Statistics	Lists Ethernet and RMON port statistics	3-116
Address Table		3-122
Static Addresses	Displays entries for interface, address or VLAN	3-122
Dynamic Addresses	Displays or edits static entries in the Address Table	3-124
Address Aging	Sets timeout for dynamically learned entries	3-125
Spanning Tree		3-126
STA		
Information	Displays STA values used for the bridge	3-127
Configuration	Configures global bridge settings for STA, RSTP and MSTP	3-131
Port Information	Displays individual port settings for STA	3-136
Trunk Information	Displays individual trunk settings for STA	3-136
Port Configuration	Configures individual port settings for STA	3-140
Trunk Configuration	Configures individual trunk settings for STA	3-140
MSTP		
VLAN Configuration	Configures priority and VLANs for a spanning tree instance	3-101
Port Information	Displays port settings for a specified MST instance	3-146

Downloaded from www.Manualslib.com manuals search engine

Menu	Description	Page
Trunk Information	Displays trunk settings for a specified MST instance	3-146
Port Configuration	Configures port settings for a specified MST instance	3-148
Trunk Configuration	Configures trunk settings for a specified MST instance	3-148
VLAN		3-150
802.1Q VLAN		
Status	Enables GVRP VLAN registration protocol	3-154
Basic Information	Displays information on the VLAN type supported by this switch	3-154
Current Table	Shows the current port members of each VLAN and whether or not the port is tagged or untagged	3-155
Static List	Used to create or remove VLAN groups	3-158
Static Table	Modifies the settings for an existing VLAN	3-159
Static Membership	Configures membership type for interfaces, including tagged, untagged or forbidden	3-161
Port Configuration	Specifies default PVID and VLAN attributes	3-163
Trunk Configuration	Specifies default trunk VID and VLAN attributes	3-163
Private VLAN		
Status	Enables or disables the private VLAN	3-167
Link Status	Configures the private VLAN	3-168
Protocol VLAN		
Configuration	Creates a protocol group, specifying the supported protocols	3-169
Port Configuration	Maps a protocol group to a VLAN	3-170
Priority		3-172
Default Port Priority	Sets the default priority for each port	3-172
Default Trunk Priority	Sets the default priority for each trunk	3-172
Traffic Classes	Maps IEEE 802.1p priority tags to output queues	3-174
Traffic Classes Status	Enables/disables traffic class priorities (not implemented)	NA

Downloaded from www.Manualslib.com manuals search engine

Menu	Description	Page
Queue Mode	Sets queue mode to strict priority or Weighted Round-Robin	3-176
Queue Scheduling	Configures Weighted Round Robin queueing	3-176
IP Precedence/ DSCP Priority Status	Globally selects IP Precedence or DSCP Priority, or disables both.	3-179
IP Precedence Priority	Sets IP Type of Service priority, mapping the precedence tag to a class-of-service value	3-181
IP DSCP Priority	Sets IP Differentiated Services Code Point priority, mapping a DSCP tag to a class-of-service value	3-183
IP Port Priority Status	Globally enables or disables IP Port Priority	3-185
IP Port Priority	Sets TCP/UDP port priority, defining the socket number and associated class-of-service value	3-185
ACL CoS Priority	Sets the CoS value and corresponding output queue for packets matching an ACL rule	3-186
ACL Marker	Change traffic priorities for frames matching an ACL rule	3-188
IGMP Snooping		3-190
IGMP Configuration	Enables multicast filtering; configures parameters for multicast query	3-193
Multicast Router Port Information	Displays the ports that are attached to a neighboring multicast router for each VLAN ID	3-195
Static Multicast Router Port Configuration	Assigns ports that are attached to a neighboring multicast router	3-196
IP Multicast Registration Table	Displays all multicast groups active on this switch, including multicast IP addresses and VLAN ID	3-198
IGMP Member Port Table	Indicates multicast addresses associated with the selected VLAN	3-199

Downloaded from www.Manualslib.com manuals search engine

Menu	Description	Page
DNS		3-206
General Configuration	Enables DNS; configures domain name and domain list; and specifies IP address of name servers for dynamic lookup	3-206
Static Host Table	Configures static entries for domain name to address mapping	3-209
Cache	Displays cache entries discovered by designated name servers	3-212
IP		3-246
General		3-250
Global Settings	Enables or disables routing, specifies the default gateway	3-250
Routing Interface	Configures the IP interface for the specified VLAN	3-252
ARP		3-255
General	Sets the protocol timeout, and enables or disables proxy ARP for the specified VLAN	3-256
Static Addresses	Statically maps a physical address to an IP address	3-257
Dynamic Addresses	Shows dynamically learned entries in the IP routing table	3-258
Other Addresses	Shows internal addresses used by the switch	3-260
Statistics	Shows statistics on ARP requests sent and received	3-261
IGMP		3-200
Interface Settings	Configures Layer 3 IGMP for specific VLAN interfaces	3-201
Group Membership	Displays the current multicast groups learned via IGMP	3-205
Statistics		3-263
IP	Shows statistics for IP traffic, including the amount of traffic, address errors, routing, fragmentation and reassembly	3-263

Downloaded from www.Manualslib.com manuals search engine

Menu	Description	Page
ICMP	Shows statistics for ICMP traffic, including the amount of traffic, protocol errors, and the number of echoes, timestamps, and address masks	3-265
UDP	Shows statistics for UDP, including the amount of traffic and errors	3-267
TCP	Shows statistics for TCP, including the amount of traffic and TCP connection activity	3-268
Routing		3-247
Static Routes	Configures and display static routing entries	3-269
Routing Table	Shows all routing entries, including local, static and dynamic routes	3-271
Multicast Routing		3-319
General Settings	Globally enables multicast routing	3-319
Multicast Routing Table	Shows each multicast route this switch has learned	3-321
VRRP		3-226
Group Configuration	Configures VRRP groups, including virtual interface address, advertisement interval, preemption, priority, and authentication	3-227
Global Statistics	Displays global statistics for VRRP protocol packet errors	3-234
Group Statistics	Displays statistics for VRRP protocol events and errors on the specified VRRP group and interface	3-235
HSRP		3-237
HSRP Group Configuration	Configures HSRP groups, including virtual interface address, advertisement interval, preemption, priority, authentication, and interface tracking	3-238
Routing Protocol		3-249
RIP		3-273
General Settings	Enables or disables RIP, sets the global RIP version and timer values	3-274
Network Addresses	Configures the network interfaces that will use RIP	3-276

Downloaded from www.Manualslib.com manuals search engine

Menu	Description	Page
Interface Settings	Configures RIP parameters for each interface, including send and receive versions, message loopback prevention, and authentication	3-277
Statistics	Displays general information on update time, route changes and number of queries, as well as a list of statistics for known interfaces and neighbors	3-281
OSPF		3-285
General Configuration	Enables or disables OSPF; also configures the Router ID and various other global settings	3-287
Area Configuration	Specifies rules for importing routes into each area	3-291
Area Range Configuration	Configures route summaries to advertise at an area boundary	3-295
Interface Configuration	Shows area ID and designated router; also configures OSPF protocol settings and authentication for each interface	3-297
Virtual Link Configuration	Configures a virtual link through a transit area to the backbone	3-303
Network Area Address Configuration	Defines OSPF areas and associated interfaces	3-305
Summary Address Configuration	Aggregates routes learned from other protocols for advertising into other autonomous systems	3-308
Redistribute Configuration	Redistributes routes from one routing domain to another	3-310
NSSA Settings	Configures settings for importing routes into or exporting routes out of not-so-stubby areas	3-311
Link State Database Information	Shows information about different OSPF Link State Advertisements (LSAs) stored in this router's database	3-313
Border Router Information	Displays routing table entries for area border routers and autonomous system boundary routers	3-316
Neighbor Information	Displays information about neighboring routers on each interface within an OSPF area	3-317

Downloaded from www.Manualslib.com manuals search engine

Menu	Description	Page
DVMRP		3-323
General Settings	Configure global settings for prune and graft messages, and the exchange of routing information	3-324
Interface Settings	Enables/disables DVMRP per interface and sets the route metric	3-329
Neighbor Information	Displays neighboring DVMRP routers	3-331
Routing Table	Displays DVMRP routing information	3-333
PIM-DM		
General Settings	Enables or disables PIM-DM globally for the switch	3-335
Interface Settings	Enables or disables PIM-DM per interface, configures protocol settings for hello, prune and graft messages	3-336
Interface Information	Displays summary information for each interface	3-339
Neighbor Information	Displays neighboring PIM-DM routers	3-340
DHCP		3-214
Relay Configuration	Specifies DHCP relay servers; enables or disables relay service	3-214
Server	Configures DHCP server parameters	3-214
General	Enables DHCP server; configures excluded address range	3-216
Pool Configuration	Configures address pools for network groups or a specific host	3-217
IP Binding	Displays addresses currently bound to DHCP clients	3-223

Downloaded from www.Manualslib.com manuals search engine

Basic Configuration

Displaying System Information

You can easily identify the system by displaying the device name, location and contact information.

Field Attributes

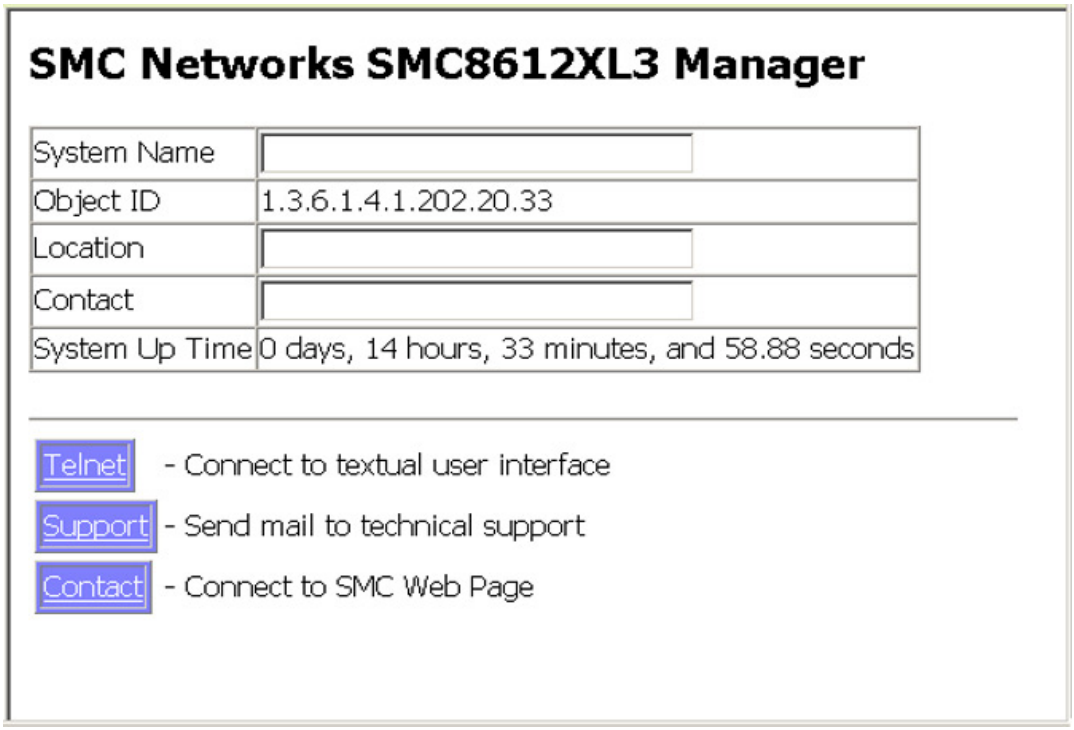
- **System Name** – Name assigned to the switch system.
- **Object ID** – MIB II object ID for switch's network management subsystem.
- **Location** – Specifies the system location.
- **Contact** – Administrator responsible for the system.
- **System Up Time** – Length of time the management agent has been up.

These additional parameters are displayed for the CLI.

- **MAC Address** – The physical layer address for this switch.
- **Web server** – Shows if management access via HTTP is enabled.
- **Web server port** – Shows the TCP port number used by the web interface.
- **Web secure server** – Shows if management access via HTTPS is enabled.
- **Web secure server port** – Shows the TCP port used by the HTTPS interface.
- **POST result** – Shows results of the power-on self-test

Web – Click System, System Information. Specify the system name, location, and contact information for the system administrator, then click Apply. (This page also includes a Telnet button that allows access to the Command Line Interface via Telnet.)

Downloaded from www.Manualslib.com manuals search engine



Downloaded from www.Manualslib.com manuals search engine

CLI – Specify the hostname, location and contact information.

```
Console(config)#hostname R&D 53-34
Console(config)#snmp-server location WC 93-149
Console(config)#snmp-server contact Ted3-148
Console(config)#exit
Console#show system3-82
System description: SMC Networks SMC8612XL3
System OID string: 1.3.6.1.4.1.202.20.33
System information
 System Up time: 0 days, 14 hours, 38 minutes, and 0.42 seconds
 System Name            : [NONE]
 System Location        : [NONE]
 System Contact         : [NONE]
 MAC address            : 00-30-F1-8F-D5-50
 Web server             : enable
 Web server port        : 80
 Web secure server      : enable
 Web secure server port : 443
 POST result
DUMMY Test 1.................PASS
UART LOOP BACK Test..........PASS
DRAM Test....................PASS
Timer Test...................PASS
PCI Device 1 Test............PASS
I2C bus Initialization.......PASS
RTC Initialization...........PASS
Switch Int Loopback test.....PASS

Done All Pass.
Console#
```

Displaying Switch Hardware/Software Versions

Use the Switch Information page to display hardware/firmware version numbers for the main board and management software, as well as the power status of the system.

Field Attributes

Main Board

- **Serial Number** – The serial number of the switch.
- **Number of Ports** – Number of built-in ports.
- **Hardware Version** – Hardware version of the main board.
- **Internal Power Status** – Displays the status of the internal power

Downloaded from www.Manualslib.com manuals search engine

supply.

- **Redundant Power Status*** – Displays the status of the redundant power supply.

* CLI only.

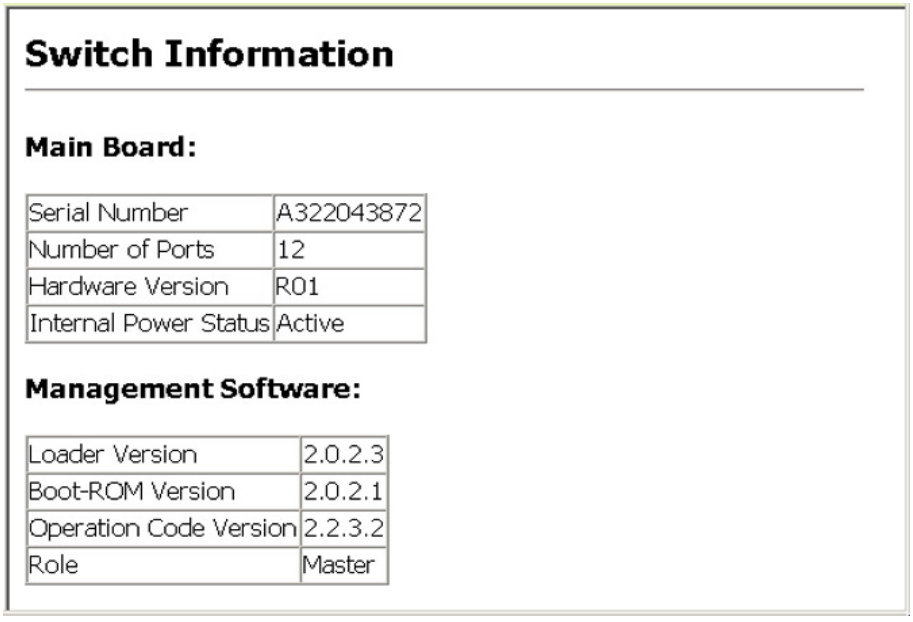
Management Software

- **Loader Version** – Version number of loader code.
- **Boot-ROM Version** – Version of Power-On Self-Test (POST) and boot code.
- **Operation Code Version** – Version number of runtime code.
- **Role** – Shows that this switch is operating as Master (i.e., operating stand-alone).

Expansion Slots

- **Expansion Slot** – Indicates any installed module type.

Web – Click System, Switch Information.



Switch Information

Main Board:

Serial Number	A322043872
Number of Ports	12
Hardware Version	R01
Internal Power Status	Active

Management Software:

Loader Version	2.0.2.3
Boot-ROM Version	2.0.2.1
Operation Code Version	2.2.3.2
Role	Master

Downloaded from www.Manualslib.com manuals search engine

CLI – Use the following command to display version information.

```
Console#show version
Unit1
 Serial number           : A322043872
 Hardware version        : R01
 Number of ports         :12
 Main power status       :up
 Redundant power status  :down
Agent (master)
 Unit ID                 : 1
 Loader version          : 2.0.2.3
 Boot ROM version        : 2.0.2.1
 Operation code version  : 2.2.3.2
Console#
```

Displaying Bridge Extension Capabilities

The Bridge MIB includes extensions for managed devices that support Multicast Filtering, Traffic Classes, and Virtual LANs. You can access these extensions to display default settings for the key variables.

Field Attributes

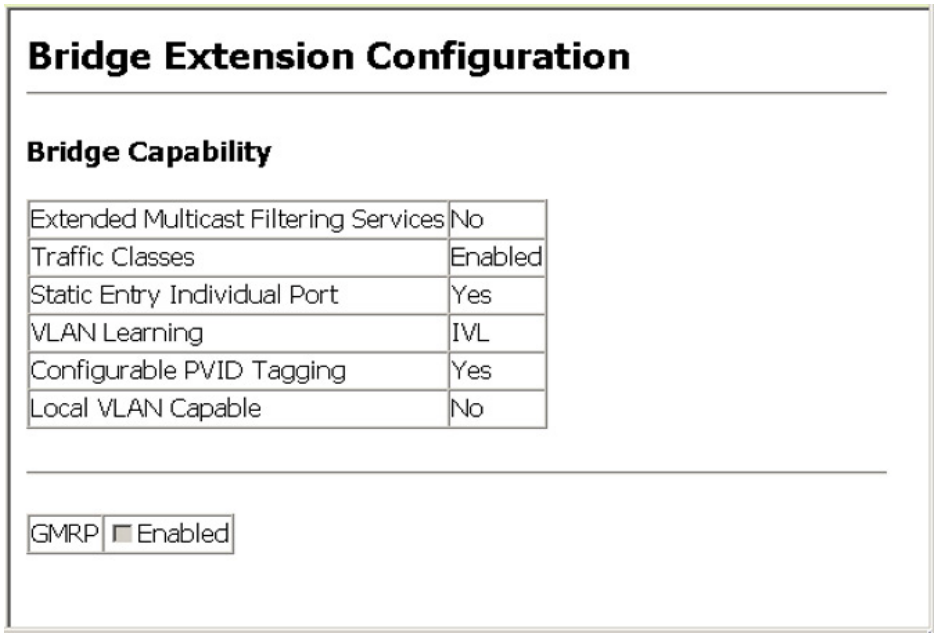
- **Extended Multicast Filtering Services** – This switch does not support the filtering of individual multicast addresses based on GMRP (GARP Multicast Registration Protocol).
- **Traffic Classes** – This switch provides mapping of user priorities to multiple traffic classes. (Refer to "Class of Service Configuration" on page 3-172.)
- **Static Entry Individual Port** – This switch allows static filtering for unicast and multicast addresses. (Refer to "Setting Static Addresses" on page 3-122.)
- **VLAN Learning** – This switch uses Independent VLAN Learning (IVL), where each port maintains its own filtering database.
- **Configurable PVID Tagging** – This switch allows you to override the default Port VLAN ID (PVID used in frame tags) and egress status (VLAN-Tagged or Untagged) on each port. (Refer to "VLAN Configuration" on page 3-150.)

Downloaded from www.Manualslib.com manuals search engine

- **Local VLAN Capable** – This switch supports multiple local bridges; i.e., multiple spanning trees. (Refer to "Configuring Multiple Spanning Trees" on page 3-101.)

- **GMRP** – GARP Multicast Registration Protocol (GMRP) allows network devices to register endstations with multicast groups. This switch does not support GMRP; it uses the Internet Group Management Protocol (IGMP) to provide automatic multicast filtering.

Web – Click System, Bridge Extension.



CLI – Enter the following command.

```
Console#show bridge-ext
 Max support VLAN numbers: 255
 Max support VLAN ID: 4094
 Extended multicast filtering services: No
 Static entry individual port: Yes
 VLAN learning: IVL
 Configurable PVID tagging: Yes
 Local VLAN capable: No
 Traffic classes: Enabled
 Global GVRP status: Disabled
 GMRP: Disabled
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Setting the Switch's IP Address

This section describes how to configure an initial IP interface for management access over the network. The IP address for this switch is unassigned by default. To manually configure an address, you need to change the switch's default settings (IP address 0.0.0.0 and netmask 255.0.0.0) to values that are compatible with your network. You may also need to a establish a default gateway between the switch and management stations that exist on another network segment (if routing is not enabled on this switch).

You can manually configure a specific IP address, or direct the device to obtain an address from a BOOTP or DHCP server. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. Anything outside this format will not be accepted by the CLI program.

Command Usage

- This section describes how to configure a single local interface for initial access to the switch. To configure multiple IP interfaces on this switch, you must set up an IP interface for each VLAN (page 3-252).
- To enable routing between the different interfaces on this switch, you must enable IP routing (page 3-250).
- To enable routing between the interfaces defined on this switch and external network interfaces, you must configure static routes (page 3-269) or use dynamic routing; i.e., either RIP (page 3-273) or OSPF (page 3-285).
- The precedence for configuring IP interfaces is the IP / General / Routing Interface menu (page 3-252), static routes (page 3-269), and then dynamic routing.

Command Attributes

- **VLAN** – ID of the configured VLAN (1-4094, no leading zeroes). By default, all ports on the switch are members of VLAN 1. However, the management station can be attached to a port belonging to any VLAN,

Downloaded from www.Manualslib.com manuals search engine

as long as that VLAN has been assigned an IP address.

- **IP Address Mode** – Specifies whether IP functionality is enabled via manual configuration (Static), Dynamic Host Configuration Protocol (DHCP), or Boot Protocol (BOOTP). If DHCP/BOOTP is enabled, IP will not function until a reply has been received from the server. Requests will be broadcast periodically by the switch for an IP address. (DHCP/BOOTP values can include the IP address, subnet mask, and default gateway.)

- **IP Address** – Address of the VLAN interface through which the management station is attached. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. (Default: 0.0.0.0)

- **Subnet Mask** – This mask identifies the host address bits used for routing to specific subnets. (Default: 255.0.0.0)

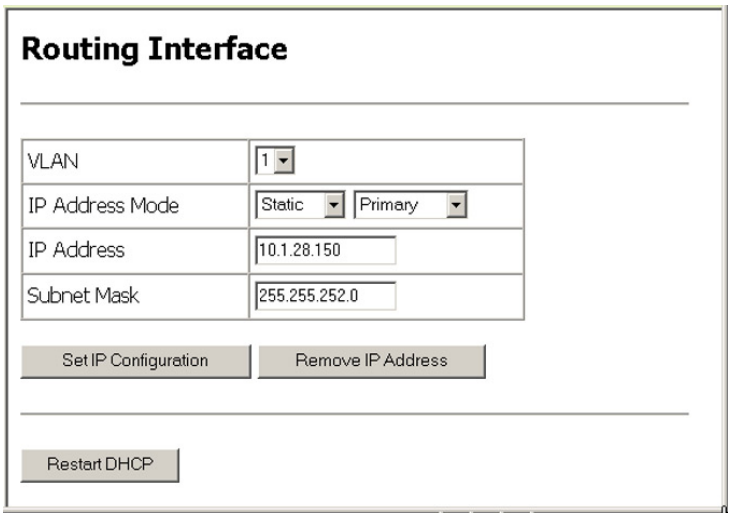
- **Default Gateway** – IP address of the gateway router between this device and management stations that exist on other network segments. (Default: 0.0.0.0)

- **MAC Address** – The physical layer address for this switch.

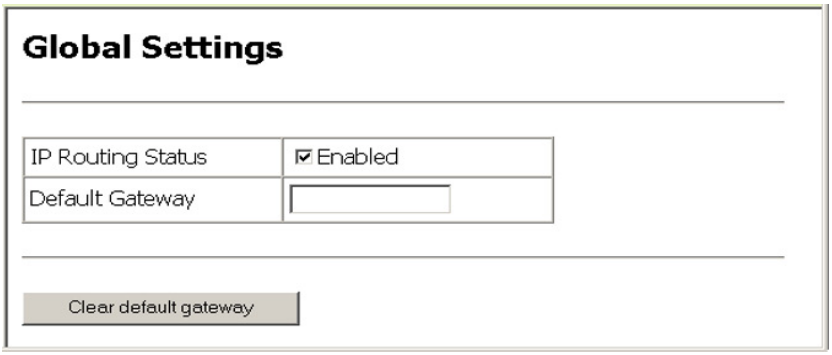
Manual Configuration

Web – Click IP, General, Routing Interface. Select the VLAN through which the management station is attached, set the IP Address Mode to "Static," and specify a "Primary" interface. Enter the IP address, subnet mask and gateway, then click Apply.

Downloaded from www.Manualslib.com manuals search engine



Click IP, Global Setting. If this switch and management stations exist on other network segments, then specify the default gateway, and click Apply.



CLI – Specify the management interface, IP address and default gateway.

```
Console#config
Console(config)#interface vlan 1
Console(config-if)#ip address 10.1.28.150 255.255.252.0
Console(config-if)#exit
Console(config)#ip default-gateway 10.1.28.149
Console(config)#
```

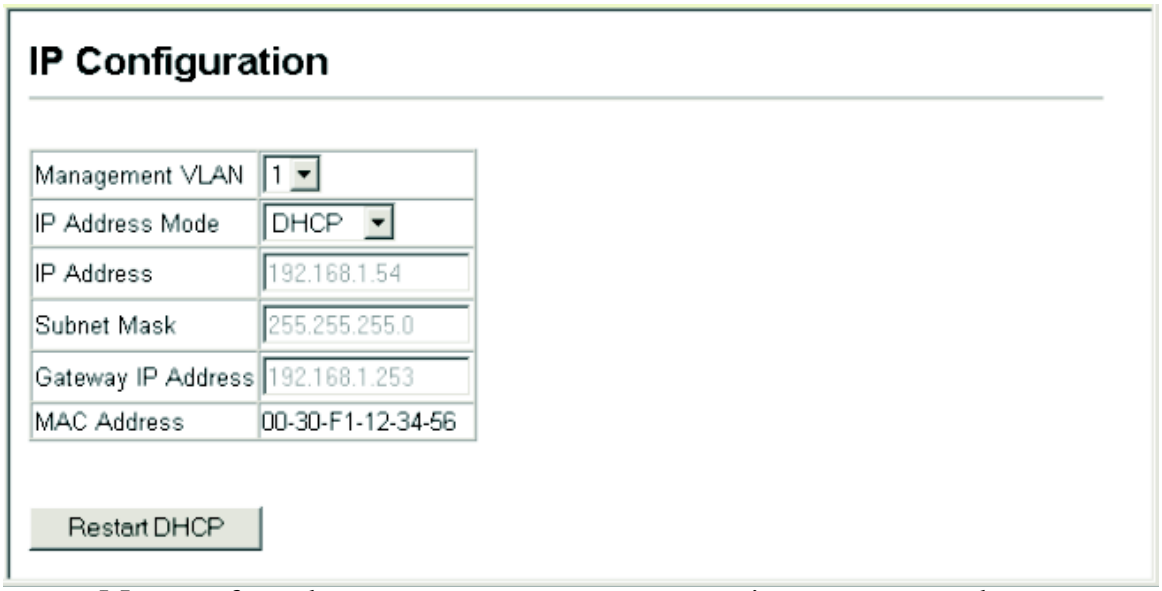
Using DHCP/BOOTP

If your network provides DHCP/BOOTP services, you can configure the switch to be dynamically configured by these services.

Web – Click IP, General, Routing Interface. Specify the VLAN to which the management station is attached, set the IP Address Mode to DHCP or

Downloaded from www.Manualslib.com manuals search engine

BOOTP. Click Apply to save your changes. Then click Restart DHCP to immediately request a new address. Note that the switch will also broadcast a request for IP configuration settings on each power reset.



Note: If you lose your management connection, use a console connection and enter "show ip interface" to determine the new switch address.

CLI – Specify the management interface, and set the IP address mode to DHCP or BOOTP, and then enter the "ip dhcp restart client" command.

```
Console#config
Console(config)#interface vlan 13-1
Console(config-if)#ip address dhcp3-116
Console(config-if)#end
Console#ip dhcp restart client3-156
Console#show ip interface3-119
 IP address and netmask: 10.1.28.150 255.255.252.0 on VLAN 1,
 and address mode: User specified.
Console#
```

Renewing DCHP – DHCP may lease addresses to clients indefinitely or for a specific period of time. If the address expires or the switch is moved to another network segment, you will lose management access to the switch. In this case, you can reboot the switch or submit a client request to restart DHCP service via the CLI.

Downloaded from www.Manualslib.com manuals search engine

Web – If the address assigned by DHCP is no longer functioning, you will not be able to renew the IP settings via the web interface. You can only restart DHCP service via the web interface if the current address is still available.

CLI – Enter the following command to restart DHCP service.

```
Console#ip dhcp restart client3-156
```

Managing Firmware

You can upload/download firmware to or from a TFTP server. By saving runtime code to a file on a TFTP server, that file can later be downloaded to the switch to restore operation. You can also set the switch to use new firmware without overwriting the previous version.

Command Attributes

- **TFTP Server IP Address** – The IP address of a TFTP server.
- **File Name** – The file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names on the TFTP server is 127 characters or 31 characters for files on the switch. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")

Note: Up to two copies of the system software (i.e., the runtime firmware) can be stored in the file directory on the switch. The currently designated startup version of this file cannot be deleted.

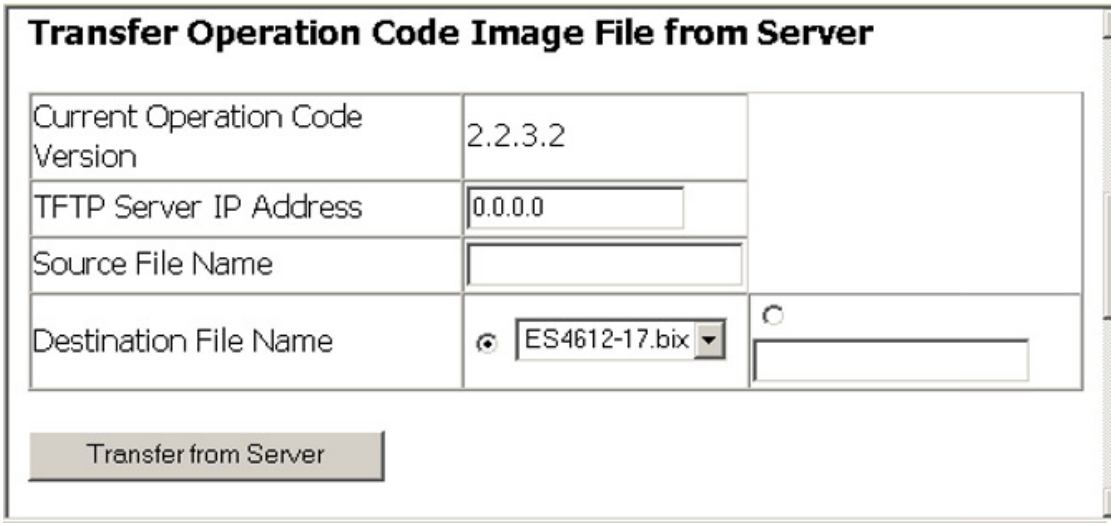
Downloading System Software from a Server

When downloading runtime code, you can specify the destination file name to replace the current image, or first download the file using a different name from the current runtime code file, and then set the new file as the startup file.

Web – Click System, Firmware. Enter the IP address of the TFTP server, enter the file name of the software to download, select a file on the switch

Downloaded from www.Manualslib.com manuals search engine

to overwrite or specify a new file name, then click Transfer from Server. To start the new firmware, reboot the system via the System/Reset menu.



If you download to a new destination file, then select the file from the drop-down box for the operation code used at startup, and click Apply Changes. To start the new firmware, reboot the system via the System/Reset menu.

Downloaded from www.Manualslib.com manuals search engine

CLI – Enter the IP address of the TFTP server, select "config" or "opcode" file type, then enter the source and destination file names, set the new file to start up the system, and then restart the switch.

```
Console#copy tftp file3-85
TFTP server ip address: 10.1.0.19
Choose file type:
 1. config:  2. opcode: <1-2>: 2
Source file name: M100000.bix
Destination file name: V1.0
\Write to FLASH Programming.
-Write to FLASH finish.
Success.
Console#config
Console(config)#boot system opcode:V1.03-91
Console(config)#exit
Console#reload3-30
```

Saving or Restoring Configuration Settings

You can upload/download configuration settings to/from a TFTP server. The configuration file can be later downloaded to restore the switch's settings.

Command Attributes

- **TFTP Server IP Address** – The IP address of a TFTP server.
- **File Name** — The configuration file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names on the TFTP server is 127 characters or 31 characters for files on the switch. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")

Note: The maximum number of user-defined configuration files is limited only by available flash memory space.

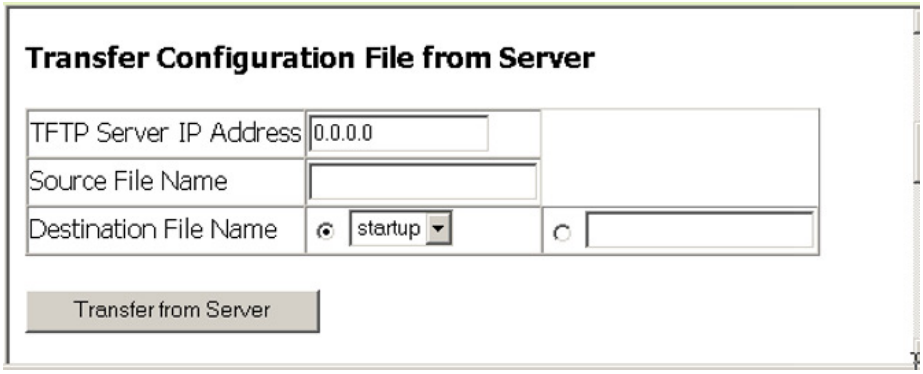
Downloading Configuration Settings from a Server

You can download the configuration file under a new file name and then set it as the startup file, or you can specify the current startup configuration file as the destination file to directly replace it. Note that the

Downloaded from www.Manualslib.com manuals search engine

file "Factory_Default_Config.cfg" can be copied to the TFTP server, but cannot be used as the destination on the switch.

Web – Click System, Configuration. Enter the IP address of the TFTP server, enter the name of the file to download, select a file on the switch to overwrite or specify a new file name, and then click Transfer from Server.



If you download to a new file name, then select the new file from the drop-down box for Startup Configuration File, and press Apply Changes. To use the new settings, reboot the system via the System/Reset menu.

CLI – Enter the IP address of the TFTP server, specify the source file on the server, set the startup file name on the switch, and then restart the switch.

```
Console#copy tftp startup-config3-85
TFTP server ip address: 192.168.1.19
Source configuration file name: config-1
Startup configuration file name [] : startup
\Write to FLASH Programming.
-Write to FLASH finish.
Success.

Console#reload
```


Downloaded from www.Manualslib.com manuals search engine

If you download the startup configuration file under a new file name, you can set this file as the startup file at a later time, and then restart the switch.

```
Console#config
Console(config)#boot system config: startup-new3-91
Console(config)#exit
Console#reload3-30
```

Configuring Event Logging

The switch allows you to control the logging of error messages, including the type of events that are recorded in switch memory, logging to a remote System Log (syslog) server, and displays a list of recent event messages.

System Log Configuration

The system allows you to enable or disable event logging, and specify which levels are logged to RAM or flash memory.

Severe error messages that are logged to flash memory are permanently stored in the switch to assist in troubleshooting network problems. Up to 4096 log entries can be stored in the flash memory, with the oldest entries being overwritten first when the available log memory (256 kilobytes) has been exceeded.

The System Logs page allows you to configure and limit system messages that are logged to flash or RAM memory. The default is for event levels 0 to 3 to be logged to flash and levels 0 to 7 to be logged to RAM.

Command Attributes

- **System Log Status** – Enables/disables the logging of debug or error messages to the logging process.

- **Flash Level** – Limits log messages saved to the switch's permanent flash memory for all levels up to the specified level. For example, if level 3 is specified, all messages from level 0 to level 3 will be logged to

Downloaded from www.Manualslib.com manuals search engine

flash. (Range: 0-7, Default: 3)

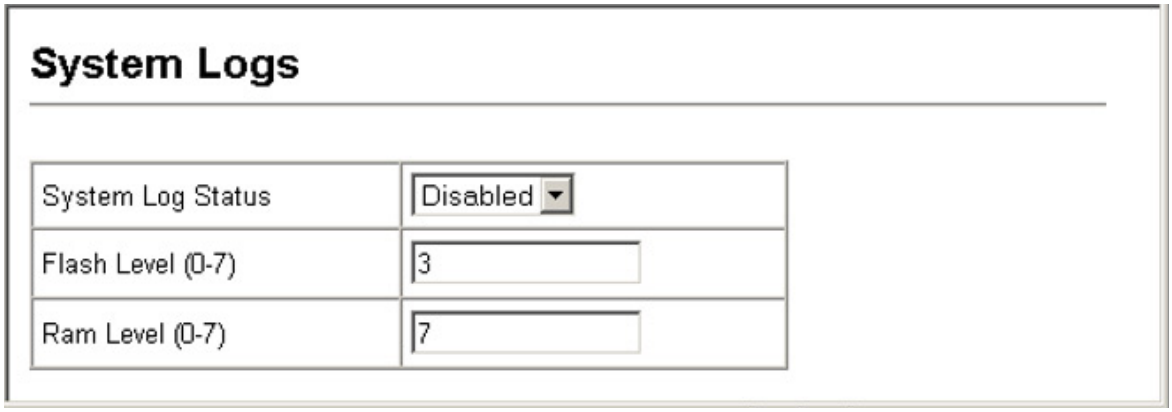
Level Argument	Level	Description
debugging	7	Debugging messages
informational	6	Informational messages only
notifications	5	Normal but significant condition, such as cold start
warnings	4	Warning conditions (e.g., return false, unexpected return)
errors	3	Error conditions (e.g., invalid input, default used)
critical	2	Critical conditions (e.g., memory allocation, or free memory error - resource exhausted)
alerts	1	Immediate action needed
emergencies	0	System unusable

* There are only Level 2, 5 and 6 error messages for the current firmware release.

- **RAM Level** – Limits log messages saved to the switch's temporary RAM memory for all levels up to the specified level. For example, if level 7 is specified, all messages from level 0 to level 7 will be logged to RAM. (Range: 0-7, Default: 7)

Note: The Flash Level must be equal to or less than the RAM Level.

Web – Click System, Logs, System Logs. Specify System Log Status, set the level of event messages to be logged, and click Apply.



Downloaded from www.Manualslib.com manuals search engine

CLI – Specify the hostname, location and contact information.

```
Console(config)#logging on3-58
Console(config)#logging history ram 03-59
Console(config)#
Console#show logging flash3-63
Syslog logging: Disable
History logging in FLASH: level errors
Console#
```

Remote Log Configuration

The Remote Logs page allows you to configure the logging of messages that are sent to syslog servers or other management stations. You can also limit the event messages sent to only those messages at or above a specified level.

Command Attributes

- **Remote Log Status** – Enables/disables the logging of debug or error messages to the remote logging process. (Default: enabled)

- **Logging Facility** – Sets the facility type for remote logging of syslog messages. There are eight facility types specified by values of 16 to 23. The facility type is used by the syslog server to dispatch log messages to an appropriate service.

  The attribute specifies the facility type tag sent in syslog messages. (See RFC 3164.) This type has no effect on the kind of messages reported by the switch. However, it may be used by the syslog server to process messages, such as sorting or storing messages in the corresponding database. (Range: 16-23, Default: 23)

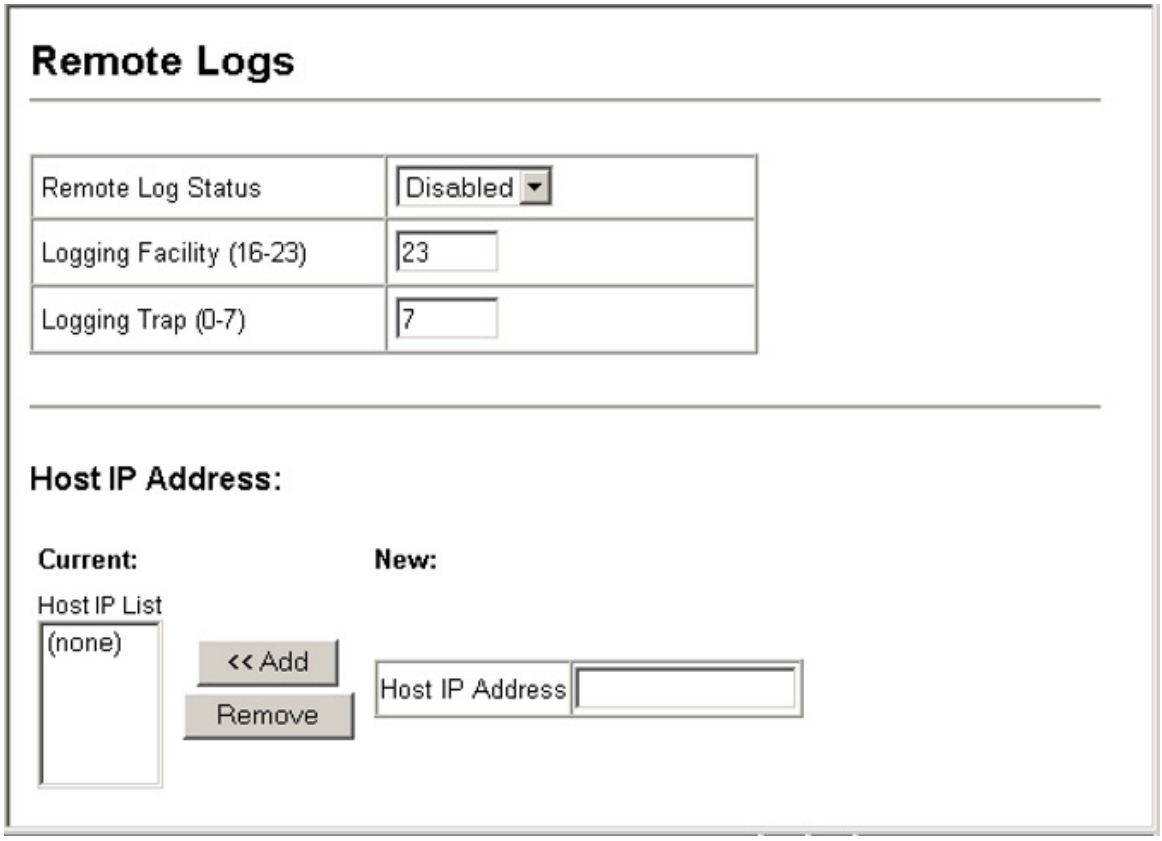
- **Logging Trap** – Limits log messages that are sent to the remote syslog server for all levels up to the specified level. For example, if level 3 is specified, all messages from level 0 to level 3 will be sent to the remote server. (Range: 0-7, Default: 3)

- **Host IP List** – Displays the list of remote server IP addresses that will receive syslog messages. The maximum number of host IP addresses allowed is five.

Downloaded from www.Manualslib.com manuals search engine

- **Host IP Address** – Specifies a new server IP address to add to the Host IP List.

Web – Click System, Remote Logs. To add an IP address to the Host IP List, type the new IP address in the Host IP Address box, and then click Add IP Host. To delete an IP address, click the entry in the Host IP List, and then click Remove Host IP.



CLI – Enter the syslog server host IP address, choose the facility type and

Downloaded from www.Manualslib.com manuals search engine

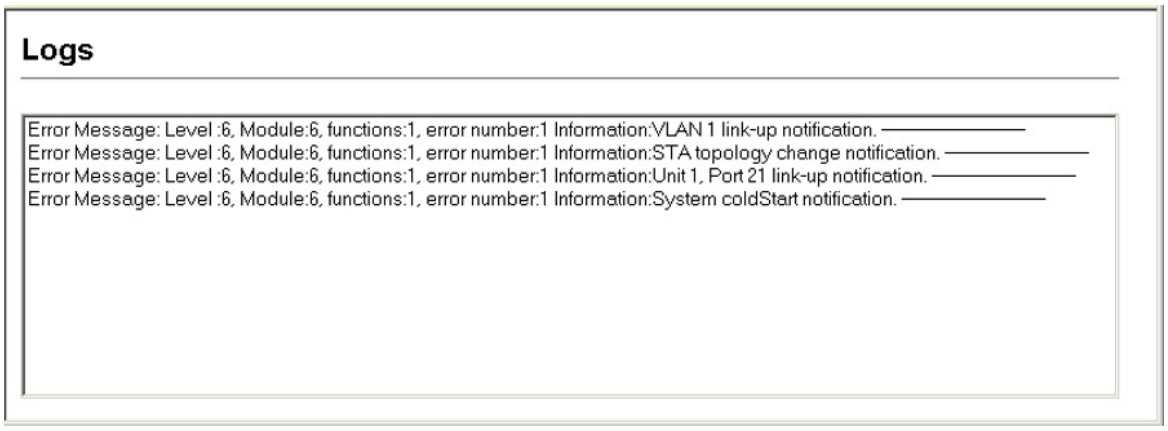
set the logging trap.

```
Console(config)#logging host 10.1.0.93-60
Console(config)#logging facility 233-61
Console(config)#logging trap 43-62
Console(config)#
Console#show logging trap3-63
Syslog logging: Enable
REMOTELOG status: enable
REMOTELOG facility type: local use 7
REMOTELOG level type: Warning conditions
REMOTELOG server ip address: 10.1.0.9
REMOTELOG server ip address: 0.0.0.0
REMOTELOG server ip address: 0.0.0.0
REMOTELOG server ip address: 0.0.0.0
REMOTELOG server ip address: 0.0.0.0
Console#
```

Displaying Log Messages

Use the Logs page to scroll through the logged system and event messages. The switch can store up to 2048 log entries in temporary random access memory (RAM; i.e., memory flushed on power reset) and up to 4096 entries in permanent flash memory.

Web – Click System, Log, Logs.


Logs
Error Message: Level :6, Module:6, functions:1, error number:1 Information:VLAN 1 link-up notification.
Error Message: Level :6, Module:6, functions:1, error number:1 Information:STA topology change notification.
Error Message: Level :6, Module:6, functions:1, error number:1 Information:Unit 1, Port 21 link-up notification.
Error Message: Level :6, Module:6, functions:1, error number:1 Information:System coldStart notification.

CLI – This example shows that system logging is enabled, the message level for flash memory is "errors" (i.e., default level 3 - 0), the message level for RAM is "debugging" (i.e., default level 7 - 0), and lists one sample

Downloaded from www.Manualslib.com manuals search engine

error .

```
Console#show logging flash3-63
Syslog logging: Enable
History logging in FLASH: level errors
[0] 0:0:5 1/1/1 "PRI_MGR_InitDefault function fails."
   level: 3, module: 13, function: 0, and event no.: 0
Console#show logging ram3-63
Syslog logging: Enable
History logging in RAM: level debugging
[0] 0:0:5 1/1/1 PRI_MGR_InitDefault function fails."
   level: 3, module: 13, function: 0, and event no.: 0
Console#
```

Resetting the System

Web – Click System, Reset. Click the Reset button to restart the switch.

CLI – Use the reload command to restart the switch.

```
Console#reload3-30
System will be restarted, continue <y/n>?
```

Note: When restarting the system, it will always run the Power-On Self-Test.

Setting the System Clock

Simple Network Time Protocol (SNTP) allows the switch to set its internal clock based on periodic updates from a time server (SNTP or NTP). Maintaining an accurate time on the switch enables the system log to record meaningful dates and times for event entries. You can also manually set the clock using the CLI. (See "calendar set" on page 3-76.) If the clock is not set, the switch will only record the time from the factory default set at the last bootup.

This switch acts as an SNTP client in two modes:

Unicast – The switch periodically sends a request for a time update to a configured time server. You can configure up to three time server IP

Downloaded from www.Manualslib.com manuals search engine

addresses. The switch will attempt to poll each server in the configured sequence.

Broadcast – The switch sets its clock from a time server in the same subnet that broadcasts time updates. If there is more than one SNTP server, the switch accepts the first broadcast it detects and ignores broadcasts from other servers.

Configuring SNTP

You can configure the switch to send time synchronization requests to specific time servers (i.e., client mode), update its clock based on broadcasts from time servers, or use both methods. When both methods are enabled, the switch will update its clock using information broadcast from time servers, but will query the specified server(s) if a broadcast is not received within the polling interval.

Command Attributes

- **SNTP Client** – Configures the switch to operate as an SNTP unicast client. This mode requires at least one time server to be specified in the SNTP Server field.

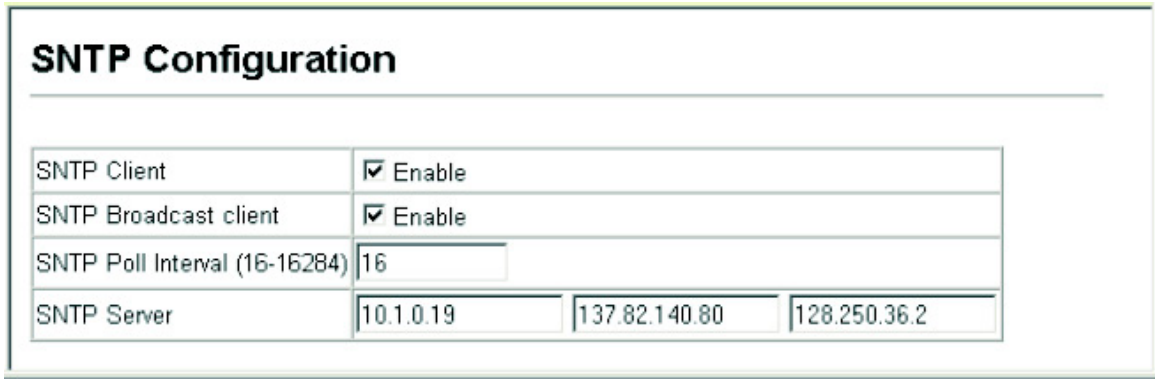
- **SNTP Broadcast Client** – Configures the switch to operate as an SNTP broadcast client. This mode requires no other configuration settings; the switch will obtain time updates from time server broadcasts (using the multicast address 224.0.1.1).

- **SNTP Poll Interval** – Sets the interval between sending requests for a time update from a time server when set to SNTP Client mode. (Range: 16-16284 seconds; Default: 16 seconds)

- **SNTP Server** – In unicast mode, sets the IP address for up to three time servers. The switch attempts to update the time from the first server, if this fails it attempts an update from the next server in the sequence.

Downloaded from www.Manualslib.com manuals search engine

Web – Select SNTP, Configuration. Modify any of the required parameters, and click Apply.



CLI – This example configures the switch to operate as an SNTP broadcast client.

```
Console(config)#sntp client3-71
Console(config)#sntp poll 163-73
Console(config)#sntp server 10.1.0.19 137.82.140.80 128.250.36.23-72
Console(config)#sntp broadcast client3-74
Console(config)#
```

Setting the Time Zone

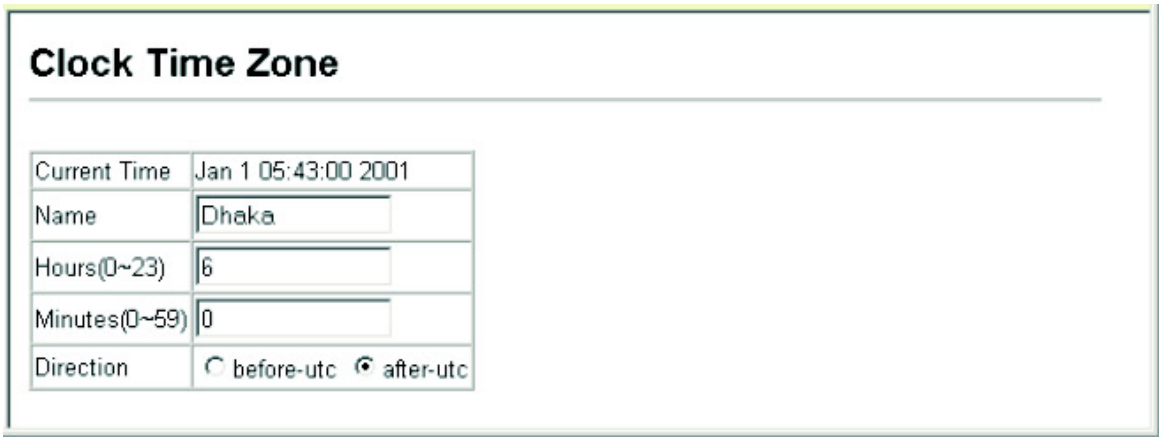
SNTP uses Coordinated Universal Time (or UTC, formerly Greenwich Mean Time, or GMT) based on the time at the Earth's prime meridian, zero degrees longitude. To display a time corresponding to your local time, you must indicate the number of hours and minutes your time zone is east (before) or west (after) of UTC.

Command Attributes

- **Current Time** – Displays the current time.
- **Name** – Assigns a name to the time zone.
- **Hours (0-12)** – The number of hours before/after UTC**.**
- **Minutes (0-59)** – The number of minutes before/after UTC.
- **Direction** – Configures the time zone to be before (east) or after (west) UTC.

Downloaded from www.Manualslib.com manuals search engine

Web – Select SNTP, Clock Time Zone. Set the offset for your time zone relative to the UTC, and click Apply.



CLI - This example shows how to set the time zone for the system clock.

```
Console(config)#clock timezone Dhaka hours 6 minute 0 after-UTC3-75
Console#
```

Simple Network Management Protocol

Simple Network Management Protocol (SNMP) is a communication protocol designed specifically for managing devices on a network. Equipment commonly managed with SNMP includes switches, routers and host computers. SNMP is typically used to configure these devices for proper operation in a network environment, as well as to monitor them to evaluate performance or detect potential problems.

The switch includes an onboard SNMP agent that continuously monitors the status of its hardware, as well as the traffic passing through its ports. A network management station can access this information using software such as HP OpenView. Access rights to the onboard agent are controlled by community strings. To communicate with the switch, the management station must first submit a valid community string for authentication. The options for configuring community strings, trap functions, and restricting access to clients with specified IP addresses are described in the following sections.

Downloaded from www.Manualslib.com manuals search engine

Setting Community Access Strings

You may configure up to five community strings authorized for management access. All community strings used for IP Trap Managers should be listed in this table. For security reasons, you should consider removing the default strings.

Command Attributes

- **SNMP Community Capability** – Indicates that the switch supports up to five community strings.

- **Community String** – A community string that acts like a password and permits access to the SNMP protocol.

Default strings: "public" (read-only access), "private" (read/write access)
Range: 1-32 characters, case sensitive

- **Access Mode**
  - **Read-Only** – Specifies read-only access. Authorized management stations are only able to retrieve MIB objects.
  - **Read/Write** – Specifies read-write access. Authorized management stations are able to both retrieve and modify MIB objects.

Web – Click SNMP, Configuration. Add new community strings as required, select the access rights from the Access Mode drop-down list, then click Add.

Downloaded from www.Manualslib.com manuals search engine

CLI – The following example adds the string "spiderman" with read/write access.

```
Console(config)#snmp-server community spiderman rw3-147
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

Specifying Trap Managers and Trap Types

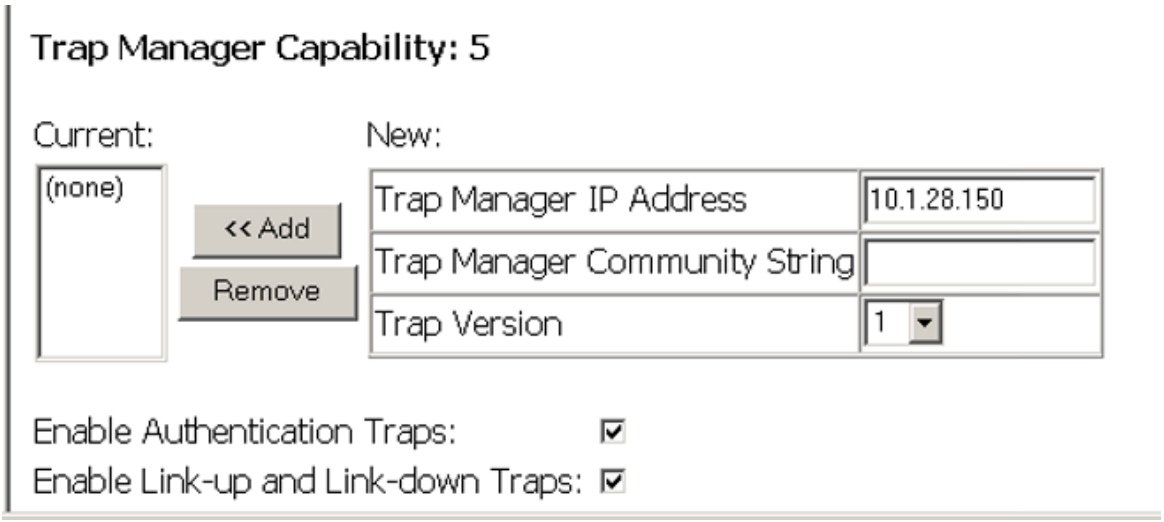
Traps indicating status changes are issued by the switch to specified trap managers. You must specify trap managers so that key events are reported by this switch to your management station (using network management platforms such as HP OpenView). You can specify up to five management stations that will receive authentication failure messages and other trap messages from the switch.

Command Attributes

- **Trap Manager Capability** – This switch supports up to five trap managers.
- **Trap Manager IP Address** – Internet address of the host (the targeted recipient).
- **Trap Manager Community String** – Community string sent with the notification operation. (Range: 1-32 characters, case sensitive)
- **Trap Version** – Specifies whether to send notifications as SNMP v1 or v2c traps.
- **Enable Authentication Traps** – Issues a trap message whenever an invalid community string is submitted during the SNMP access authentication process.
- **Enable Link-up and Link-down Traps** – Issues a trap message whenever a port link is established or broken. (Default: Enabled)

Web – Click SNMP, Configuration. Fill in the IP address and community string for each trap manager that will receive these messages, specify the SNMP version, mark the trap types required, and then click Add.

Downloaded from www.Manualslib.com manuals search engine



CLI – This example adds a trap manager and enables both authentication and link-up, link-down traps.

```
Console(config)#snmp-server host 10.1.28.150 private version 2c3-150
Console(config)#snmp-server enable traps3-151
```


Downloaded from www.Manualslib.com manuals search engine

Filtering Addresses for SNMP Client Access

The switch allows you to create a list of up to 16 IP addresses or IP address groups that are allowed access to the switch via SNMP management software (also see page 3-69).

Command Usage

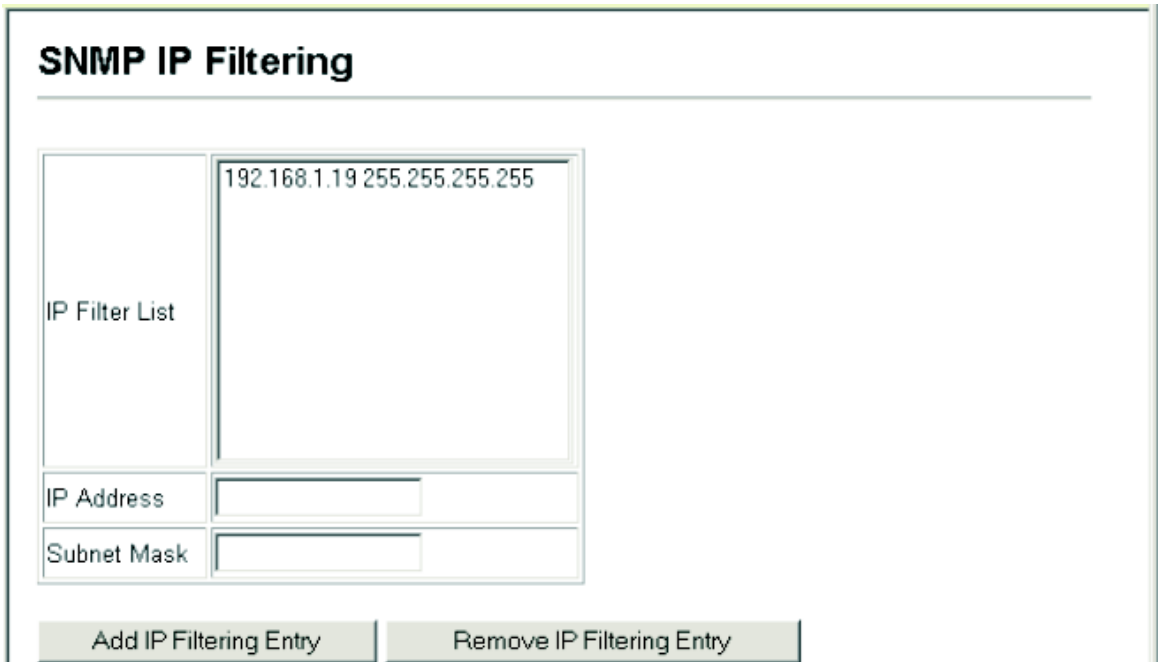
- To specify the clients allowed SNMP access, enter an IP address along with a subnet mask to identify a specific host or a range of valid addresses. For example:
  - IP address 192.168.1.1 and mask 255.255.255.255 – Specifies a valid IP address of 192.168.1.1 for a single client.
  - IP address 192.168.1.1 and mask 255.255.255.0 – Specifies a valid IP address group from 192.168.1.0 to 192.168.1.254.
- IP filtering only restricts management access for clients running SNMP management software such as HP OpenView. It does not affect management access to the switch using the web interface or Telnet.
- The default setting is null, which allows all IP groups SNMP access to the switch. If one or more IP addresses are configured, IP filtering is enabled and only addresses listed in this table will have SNMP access.

Command Attributes

- **IP Filter List** – Displays a list of the IP address/subnet mask entries currently configured for SNMP access.
- **IP address** – Specifies a new IP address to add to the IP Filter List.
- **Subnet Mask** – Specifies a single IP address or group of addresses. If the IP is the address of a single management station, set the mask to 255.255.255.255. Otherwise, an IP address group will be specified by any other mask.

Downloaded from www.Manualslib.com manuals search engine

Web – Click SNMP, IP Filtering. To add a client, enter the new address, the subnet mask for a node or an address range, and then click "Add IP Filtering Entry."



CLI – This example allows SNMP access for a specific client.

```
Console(config)#snmp ip filter 10.1.2.3 255.255.255.255
Console(config)#
```

3-152

User Authentication

You can restrict management access to this switch using the following options:

- Passwords – Manually configure access rights on the switch for specified users.
- Authentication Settings – Use remote authentication to configure access rights.
- HTTPS Settings – Provide a secure web connection.
- SSH Settings – Provide a secure shell (for secure Telnet access).
- Port Security – Configure secure addresses for individual ports.

Downloaded from www.Manualslib.com manuals search engine

- 802.1x – Use IEEE 802.1x port authentication to control access to specific ports.

Configuring the Logon Password

The guest only has read access for most configuration parameters. However, the administrator has write access for all parameters governing the onboard agent. You should therefore assign a new administrator password as soon as possible, and store it in a safe place.

The default guest name is "guest" with the password "guest." The default administrator name is "admin" with the password "admin." Note that user names can only be assigned via the CLI.

Command Attributes

- **User Name*** – The name of the user.

(Maximum length: 8 characters)

- **Access Level*** – Specifies the user level.

(Options: Normal and Privileged)

- **Password** – Specifies the user password.

(Range: 0-8 characters plain text, case sensitive)

* CLI only.

Web – Click Security, Passwords. To change the password for the current user, enter the old password, the new password, confirm it by entering it again, then click Apply.

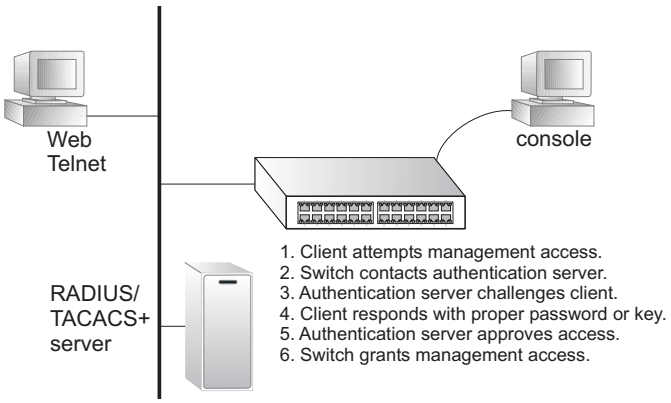
Downloaded from www.Manualslib.com manuals search engine

CLI – Assign a user name to access-level 15 (i.e., administrator), then specify the password.

```
Console(config)#username bob access-level 15
Console(config)#username bob password 0 smith
Console(config)#
```

Configuring Local/Remote Logon Authentication

Use the Authentication Settings menu to restrict management access based on specified user names and passwords. You can manually configure access rights on the switch, or you can use a remote access authentication server based on RADIUS or TACACS+ protocols.



Remote Authentication Dial-in User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+) are logon authentication protocols that use software running on a central server to control access to RADIUS-aware or TACACS- aware devices on the network. An authentication server contains a database of multiple user name/password pairs with associated privilege levels for each user that requires management access to the switch.

RADIUS uses UDP while TACACS+ uses TCP. UDP only offers best effort delivery, while TCP offers a connection-oriented transport. Also, note that RADIUS encrypts only the password in the access-request packet from the client to the server, while TACACS+ encrypts the entire body of the packet.

Command Usage

- By default, management access is always checked against the authentication database stored on the local switch. If a remote authentication server is used, you must specify the authentication

Downloaded from www.Manualslib.com manuals search engine

sequence and the corresponding parameters for the remote authentication protocol. Local and remote logon authentication control management access via the console port, web browser, or Telnet.

- RADIUS and TACACS+ logon authentication assign a specific privilege level for each user name/password pair. The user name, password, and privilege level must be configured on the authentication server.

- You can specify up to three authentication methods for any user to indicate the authentication sequence. For example, if you select (1) RADIUS, (2) TACACS and (3) Local, the user name and password on the RADIUS server is verified first. If the RADIUS server is not available, then authentication is attempted using the TACACS+ server, and finally the local user name and password is checked.

Command Attributes

- **Authentication** – Select the authentication, or authentication sequence required:

  - **Local** – User authentication is performed only locally by the switch.
  - **Radius** – User authentication is performed using a RADIUS server only.
  - **TACACS** – User authentication is performed using a TACACS+ server only.
  - [authentication sequence] – User authentication is performed by up to three authentication methods in the indicated sequence.

- **RADIUS Settings**

  - **Server IP Address** – Address of authentication server. (Default: 10.1.0.1)

  - **Server Port Number** – Network (UDP) port of authentication server used for authentication messages. (Range: 1-65535; Default: 1812)

Downloaded from www.Manualslib.com manuals search engine

- **Secret Text String** – Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 20 characters)
- **Number of Server Transmits** – Number of times the switch tries to authenticate logon access via the authentication server. (Range: 1-30; Default: 2)
- **Timeout for a reply** – The number of seconds the switch waits for a reply from the RADIUS server before it resends the request. (Range: 1-65535; Default: 5)

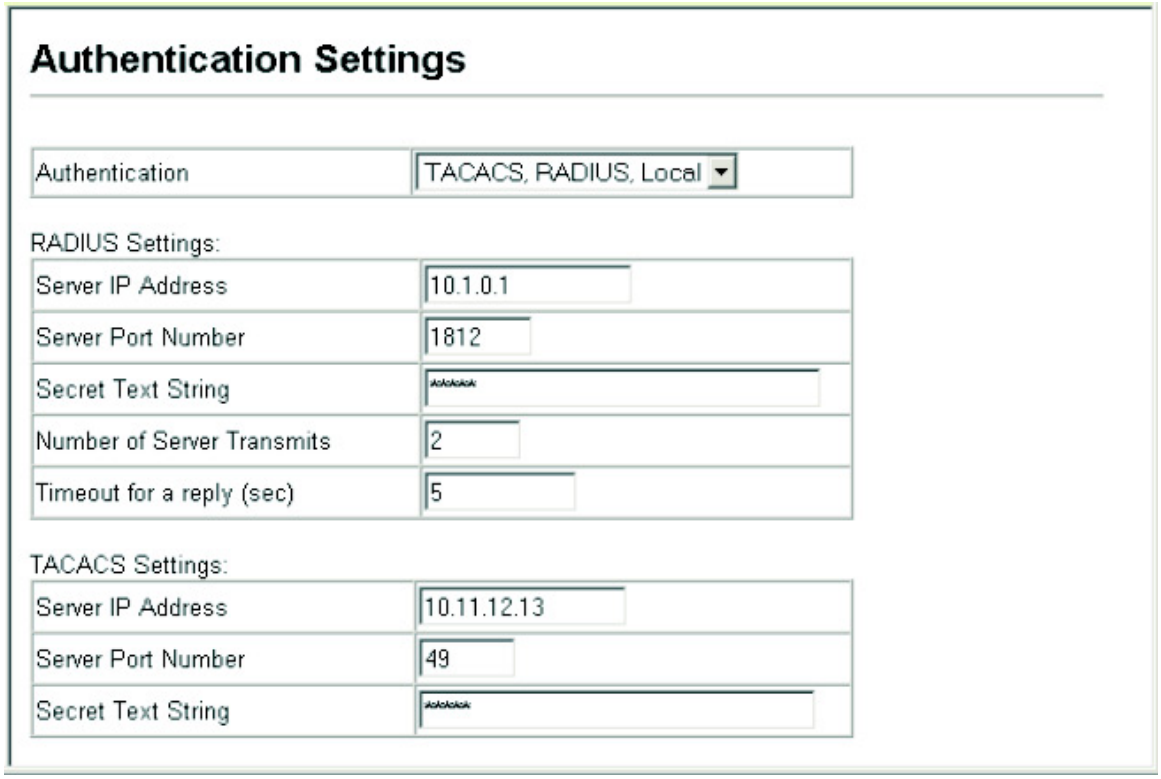
• **TACACS Settings**

- **Server IP Address** – Address of the TACACS+ server. (Default: 10.11.12.13)
- **Server Port Number** – Network (TCP) port of TACACS+ server used for authentication messages. (Range: 1-65535; Default: 49)
- **Secret Text String** – Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 20 characters)

Note: The local switch user database has to be set up by manually entering user names and passwords using the CLI. (See "username" on page 3-35.)

Web – Click Security, Authentication Settings. To configure local or remote authentication preferences, specify the authentication sequence (i.e., one to three methods), fill in the parameters for RADIUS or TACACS+ authentication if selected, and click Apply.

Downloaded from www.Manualslib.com manuals search engine



CLI – Specify all the required parameters to enable logon authentication.

```
Console(config)#authentication login radius3-93
Console(config)#radius-server host 192.168.1.253-95
Console(config)#radius-server port 1813-95
Console(config)#radius-server key green3-96
Console(config)#radius-server retransmit 53-96
Console(config)#radius-server timeout 103-97
Console#show radius-server3-97
Server IP address: 192.168.1.25
 Communication key with radius server:
 Server port number: 181
 Retransmit times: 5
 Request timeout: 10
Console(config)#authentication login tacacs3-93
Console(config)#tacacs-server host 10.20.30.403-98
Console(config)#tacacs-server port 2003-99
Console(config)#tacacs-server key green3-99
Console#show tacacs-server3-100
Server IP address: 10.20.30.40
 Communication key with tacacs server: green
 Server port number: 200
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

Configuring HTTPS

You can configure the switch to enable the Secure Hypertext Transfer Protocol (HTTPS) over the Secure Socket Layer (SSL), providing secure access (i.e., an encrypted connection) to the switch's web interface.

Command Usage

- Both the HTTP and HTTPS service can be enabled independently on the switch. However, you cannot configure both services to use the same UDP port.
- If you enable HTTPS, you must indicate this in the URL that you specify in your browser: https://*device*[:*port_number*]
- When you start HTTPS, the connection is established in this way:
  - The client authenticates the server using the server's digital certificate.
  - The client and server negotiate a set of security protocols to use for the connection.
  - The client and server generate session keys for encrypting and decrypting data.
- The client and server establish a secure encrypted connection. A padlock icon should appear in the status bar for Internet Explorer 5.x or above and Netscape Navigator 4.x or above.
- The following web browsers and operating systems currently support HTTPS:

Web Browser	Operating System
Internet Explorer 5.0 or later	Windows 98,Windows NT (with service pack 6a), Windows 2000, Windows XP
Netscape Navigator 4.76 or later	Windows 98,Windows NT (with service pack 6a), Windows 2000, Windows XP, Solaris 2.6

- To specify a secure-site certificate, see "Replacing the Default

Downloaded from www.Manualslib.com manuals search engine

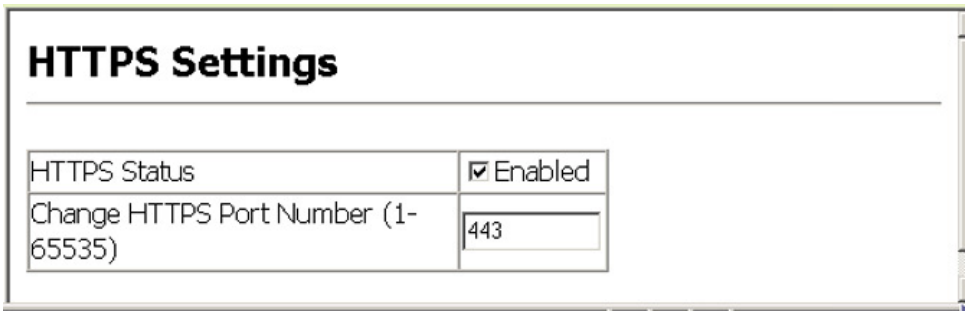
Secure-site Certificate" on page 3-49.

Command Attributes

- **HTTPS Status** – Allows you to enable/disable the HTTPS server feature on the switch. (Default: Enabled)

- **Change HTTPS Port Number** – Specifies the UDP port number used for HTTPS/SSL connection to the switch's web interface. (Default: Port 443)

Web – Click Security, HTTPS Settings. Enable HTTPS and specify the port number, then click Apply.



CLI – This example enables the HTTP secure server and modifies the port number.

```
Console(config)#ip http secure-server3-42
Console(config)#ip http secure-port 4433-44
Console(config)#
```

Replacing the Default Secure-site Certificate

When you log onto the web interface using HTTPS (for secure access), a Secure Sockets Layer (SSL) certificate appears for the switch. By default, the certificate that Netscape and Internet Explorer display will be associated with a warning that the site is not recognized as a secure site. This is because the certificate has not been signed by an approved certification authority. If you want this warning to be replaced by a message confirming that the connection to the switch is secure, you must obtain a unique certificate and a private key and password from a recognized certification authority.

Downloaded from www.Manualslib.com manuals search engine

Caution: For maximum security, we recommend you obtain a unique Secure Sockets Layer certificate at the earliest opportunity. This is because the default certificate for the switch is not unique to the hardware you have purchased.

When you have obtained these, place them on your TFTP server, and use the following command at the switch's command-line interface to replace the default (unrecognized) certificate with an authorized one:

```
Console#copy tftp https-certificate3-85
TFTP server ip address: <server ip-address>
Source certificate file name: <certificate file name>
Source private file name: <private key file name>
Private password: <password for private key>
```

Note: The switch must be reset for the new certificate to be activated. To reset the switch, type "reload" at the command prompt:

```
Console#reload
```

Configuring the Secure Shell

The Berkley-standard includes remote access tools originally designed for Unix systems. Some of these tools have also been implemented for Microsoft Windows and other environments. These tools, including commands such as *rlogin* (remote login), *rsh* (remote shell), and *rcp* (remote copy), are not secure from hostile attacks.

The Secure Shell (SSH) includes server/client applications intended as a secure replacement for the older Berkley remote access tools. SSH can also provide remote management access to this switch as a secure replacement for Telnet. When the client contacts the switch via the SSH protocol, the switch generates a public-key that the client uses along with a local user name and password for access authentication. SSH also encrypts all data transfers passing between the switch and SSH-enabled management station clients, and ensures that data traveling over the network arrives unaltered.

Note that you need to install an SSH client on the management station to access the switch for management via the SSH protocol.

Downloaded from www.Manualslib.com manuals search engine

Note: The switch supports both SSH Version 1.5 and 2.0.

Command Usage

The SSH server on this switch supports both password and public key authentication. If password authentication is specified by the SSH client, then the password can be authenticated either locally or via a RADIUS or TACACS+ remote authentication server, as specified on the **Authentication Settings** page (page 3-44). If public key authentication is specified by the client, then you must configure authentication keys on both the client and the switch as described in the following section. Note that regardless of whether you use public key or password authentication, you still have to generate authentication keys on the switch (SSH Host Key Settings) and enable the SSH server (Authentication Settings).

To use the SSH server, complete these steps:

1. *Generate a Host Key Pair* – On the SSH Host Key Settings page, create a host public/private key pair.

2. *Provide Host Public Key to Clients* – Many SSH client programs automatically import the host public key during the initial connection setup with the switch. Otherwise, you need to manually create a known hosts file on the management station and place the host public key in it. An entry for a public key in the known hosts file would appear similar to the following example:

   10.1.0.54 1024 35 15684995401867669259333946775054617325313674890836547254
   15020245593199868544358361651999923329781766065830956 10825913212890233
   76546801726272571413428762941301196195566782 59566410486957427888146206
   51941746772984865468615717739390164779355942303577413098022737087794545240839
   71752646358058176716709574804776117

3. *Import Client's Public Key to the Switch* – Use the **copy tftp public-key** command (page 3-85) to copy a file containing the public key for all the SSH client's granted management access to the switch. The clients are subsequently authenticated using these keys. The current firmware only accepts public key files based on standard UNIX format as

Downloaded from www.Manualslib.com manuals search engine

shown in the following example:

```
1024 35 134108168560989392104094492015542534763164192187295892114317388
0555361616310517759408386863110929123222682851925437460310093718772119969631
7813662774141689851320491172048303392543241016379975923714490119380060902539
4084827178194372288402533115952134861022902978982721353267131629432532818915
045306393916643 steve@192.168.1.19
```

4. *Set the Optional Parameters* – On the SSH Settings page, configure the optional parameters, including the authentication timeout, the number of retries, and the server key size.

5. *Enable SSH Service* – On the SSH Settings page, enable the SSH server on the switch.

6. *Challenge-Response Authentication* – When an SSH client attempts to contact the switch, the SSH server uses the host key pair to negotiate a session key and encryption method. Only clients that have a private key corresponding to the public keys stored on the switch can access it. The following exchanges take place during this process:

a. The client sends its public key to the switch.
b. The switch compares the client's public key to those stored in memory.
c. If a match is found, the switch uses the public key to encrypt a random sequence of bytes, and sends this string to the client.
d. The client uses its private key to decrypt the bytes, and sends the decrypted bytes back to the switch.
e. The switch compares the decrypted bytes to the original bytes it sent. If the two sets match, this means that the client's private key corresponds to an authorized public key, and the client is authenticated.

Notes: **1.** To use SSH with only password authentication, the host public key must still be given to the client, either during initial connection or manually entered into the known host file. However, you do not need to configure the client's keys.

2. The SSH server supports up to four client sessions. The maximum number of client sessions includes both current

Downloaded from www.Manualslib.com manuals search engine

Telnet sessions and SSH sessions.

Generating the Host Key Pair

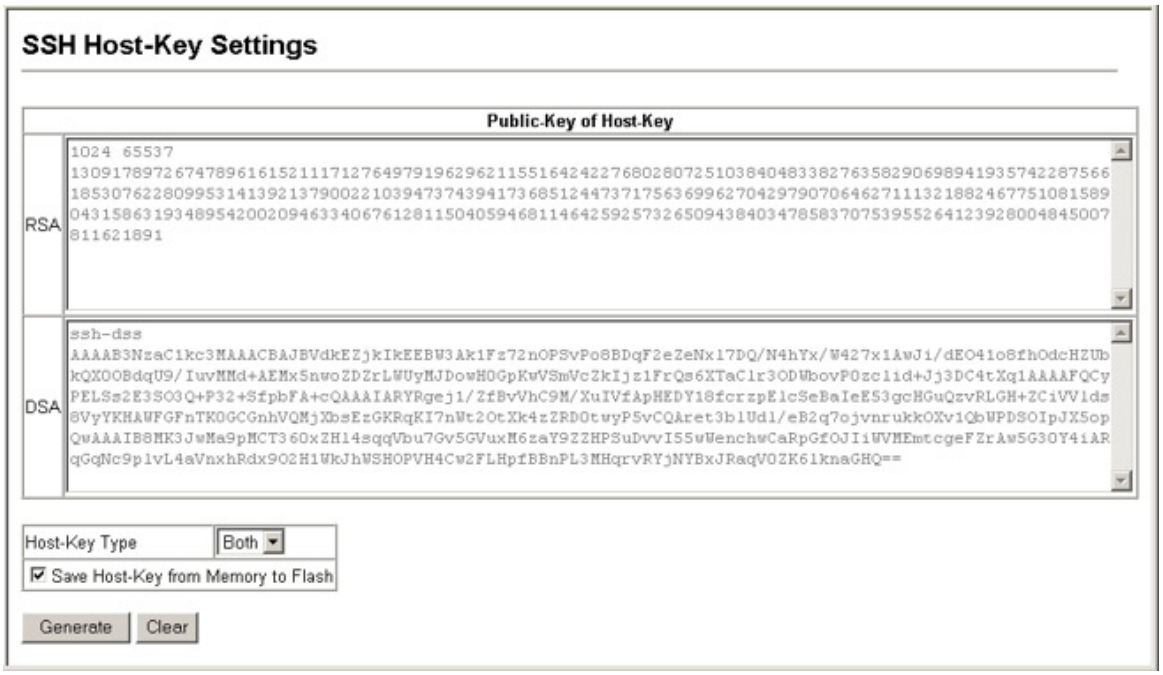
A host public/private key pair is used to provide secure communications between an SSH client and the switch. After generating this key pair, you must provide the host public key to SSH clients and import the client's public key to the switch as described in the preceeding section (Command Usage).

Field Attributes

- **Public-Key of Host-Key** – The public key for the host.
  - RSA: The first field indicates the size of the host key (e.g., 1024), the second field is the encoded public exponent (e.g., 65537), and the last string is the encoded modulus.
  - DSA: The first field indicates that the encryption method used by SSH is based on the Digital Signature Standard (DSS). The last string is the encoded modulus.
- **Host-Key Type** – The key type used to generate the host key pair (i.e., public and private keys). (Range: RSA, DSA, Both: Default: RSA)
  The SSH server uses RSA or DSA for key exchange when the client first establishes a connection with the switch, and then negotiates with the client to select either DES (56-bit) or 3DES (168-bit) for data encryption.
- **Save Host-Key from Memory to Flash** – Saves the host key from RAM (i.e., volatile memory to flash memory). Otherwise, the host key pair is stored to RAM by default. Note that you must select this item prior to generating the host-key pair.
- **Generate** – This button is used to generate the host key pair. Note that you must first generate the host key pair before you can enable the SSH server on the SSH Server Settings page.

Downloaded from www.Manualslib.com manuals search engine

Web – Click Security, Host-Key Settings. Select the host-key type from the drop-down box, select the option to save the host key from memory to flash (if required) prior to generating the key, and then click Generate.



CLI – This example generates a host-key pair using both the RSA and DSA algorithms, stores the keys to flash memory, and then displays the host's public keys.

```
Console#ip ssh crypto host-key generate3-48
Console#ip ssh save host-key3-48
Console#show public-key host3-48
Host:
RSA:
1024 65537 12725092254492640213133651454613118967905519236007602865300676182409690947448320102524878965977592168322225584652387791546479807396314033869257931051057652122430528078658854857892726029378660892368414232759121276032591968369705343933643844522333518828717389689451172929051081391964202519093210432857904576489 1
DSA:
ssh-dss AAAAB3NzaC1kc3MAAACBAN6zwIqCqDb3869jYVXlME1sHL0EcE/Re6hlasfEthIwmjhLY4O0jqJZpcEQUgCfYlum0Y2uoLka+Py9ieGWQ8f2gobUZKIICuKg6vjO9XTs7XKc05xfzkBiKviDa+2OrIz6UK+6vFOgvUDFedlnixYTVo+h5v8r0ea2rpnO6DkZAAAAFQCNZn/x17dwpW8RrVDQnSWw4Qk+6QAAAIEAptkGeB6B5hwagH4gUOCY6i1TmrmSiJgfwO9OqRPUMbCAkCC+uzxatOo7drnIZypMx+Sx5RUdMGgKS+9ywsa1cWqHeFY5ilc3lDCNBueeLykZzVS+RS+azTKIk/zrJh8GLGNq375R55yRxFvmcGIn/Q7IphPqyJ3o9MK8LFDfmJEAAACAL8A6tESiswP2OFqX7VGoEbzVDSOIRTMFy3iUXtvGyQAOVSy67Mfc3lMtgqPRUOYXDiwIBp5NXgilCg5z7VqbmRm28mWc5a//f8TUAgPNWKV6W0hqmshQdotVzDR1e+XKNTZj0uTwWfjO5Kytdn4MdoTHgrbl/DMdAfjnte8MZZs=

Console#
```


Downloaded from www.Manualslib.com manuals search engine

Configuring the SSH Server

The SSH server includes basic settings for authentication.

Field Attributes

- **SSH Server Status** – Allows you to enable/disable the SSH server on the switch. (Default: Enabled)

- **Version** – The Secure Shell version number. Version 2.0 is displayed, but the switch supports management access via either SSH Version 1.5 or 2.0 clients.

- **SSH Authentication Timeout** – Specifies the time interval in seconds that the SSH server waits for a response from a client during an authentication attempt.
  (Range: 1 to 120 seconds; Default: 120 seconds)

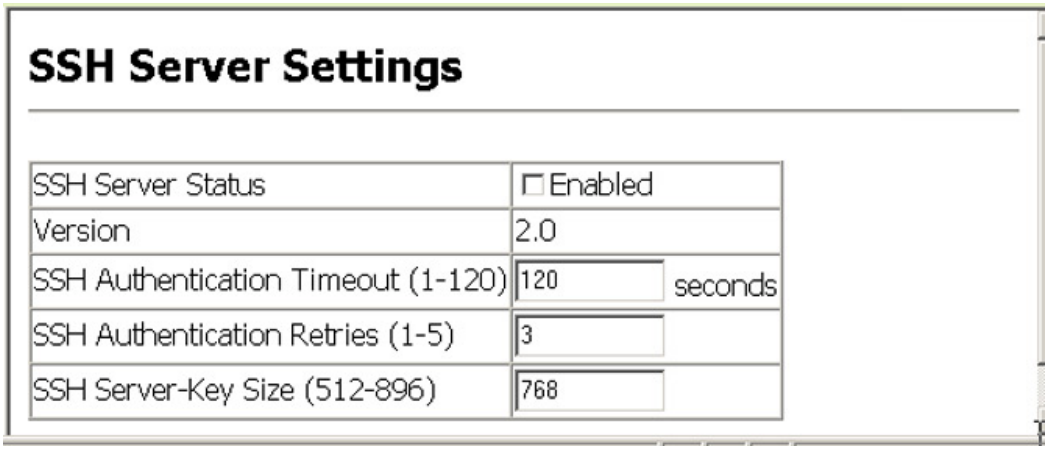
- **SSH Authentication Retries** – Specifies the number of authentication attempts that a client is allowed before authentication fails and the client has to restart the authentication process. (Range: 1-5 times; Default: 3)

- **SSH Server-Key Size** – Specifies the SSH server key size. (Range: 512-896 bits)

  - The server key is a private key that is never shared outside the switch.
  - The host key is shared with the SSH client, and is fixed at 1024 bits.

Web – Click Security, SSH, Settings. Enable SSH and adjust the authentication parameters as required, then click Apply. Note that you must first generate the host key pair on the SSH Host-Key Settings page before you can enable the SSH server.

Downloaded from www.Manualslib.com manuals search engine



CLI – This example enables SSH, sets the authentication parameters, and displays the current configuration. It shows that the administrator has made a connection via SHH, and then disables this connection.

```
Console(config)#ip ssh server3-48
Console(config)#ip ssh timeout 1203-49
Console(config)#ip ssh authentication-retries 33-50
Console(config)#ip ssh server-key size 7683-51
Console(config)#end
Console#show ip ssh3-54
SSH Enabled - version 2.0
Negotiation timeout: 120 secs; Authentication retries: 3
Server key size: 768 bits
Console#show ssh3-55
Information of secure shell
Session Username Version Encrypt method Negotiation state
------- -------- ------- -------------- -----------------
      0    admin   2.0      cipher-3des   session-started
Console#disconnect 03-25
Console#
```

Configuring Port Security

Port security is a feature that allows you to configure a switch port with one or more device MAC addresses that are authorized to access the network through that port.

When port security is enabled on a port, the switch stops learning new MAC addresses on the specified port. Only incoming traffic with source addresses already stored in the dynamic or static address table will be accepted as authorized to access the network through that port. If a device with an unauthorized MAC address attempts to use the switch port, the

Downloaded from www.Manualslib.com manuals search engine

intrusion will be detected and the switch can automatically take action by disabling the port and sending a trap message.

To use port security, first allow the switch to dynamically learn the <source MAC address, VLAN> pair for frames received on a port for an initial training period, and then enable port security to stop address learning. Be sure you enable the learning function long enough to ensure that all valid VLAN members have been registered on the selected port. Note that you can also restrict the maximum number of addresses that can be learned by a port.

To add new VLAN members at a later time, you can manually add secure addresses with the Static Address Table (page 3-122), or turn off port security to reenable the learning function long enough for new VLAN members to be registered. Learning may then be disabled again, if desired, for security.

Command Usage

- A secure port has the following restrictions:
  - Cannot use port monitoring.
  - Cannot be a multi-VLAN port.
  - It cannot be used as a member of a static or dynamic trunk.
  - It should not be connected to a network interconnection device.
- If a port is disabled (shut down) due to a security violation, it must be manually re-enabled from the Port/Port Configuration page (page 3-93).

Command Attributes

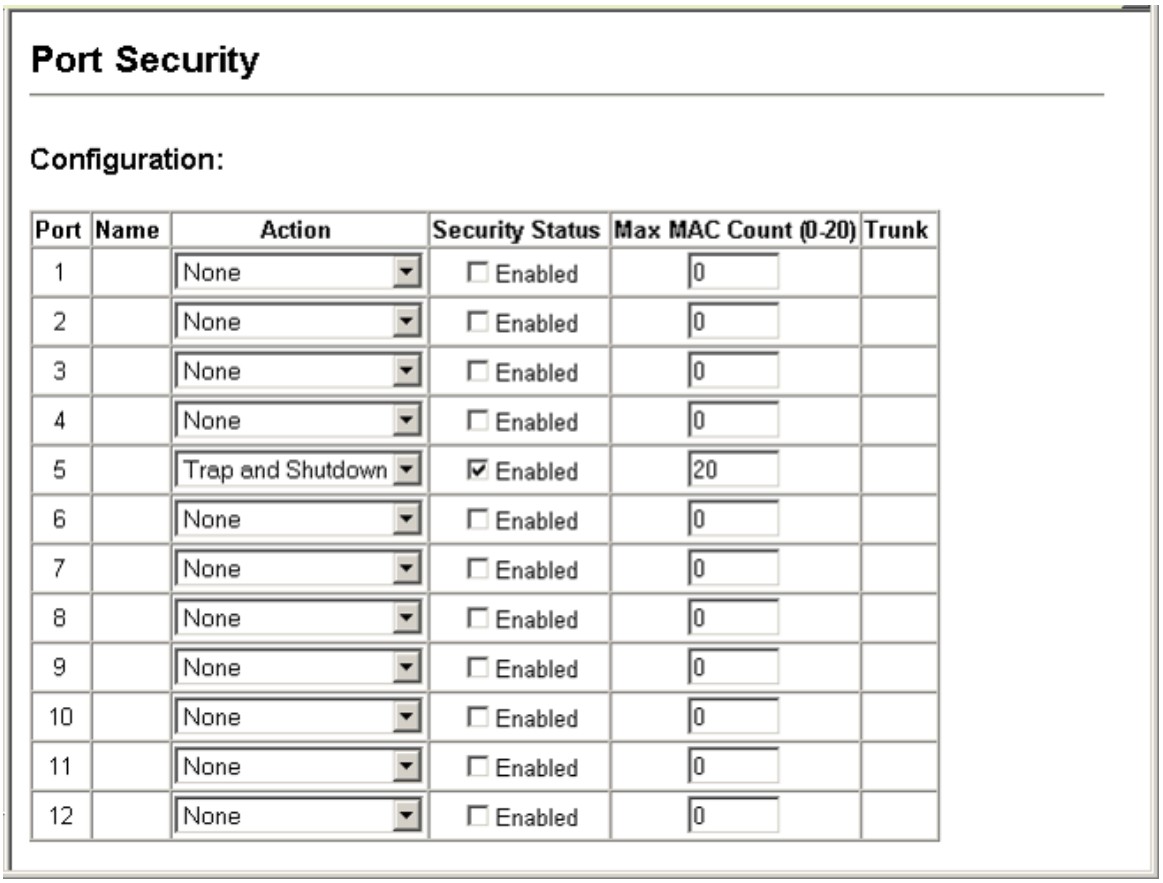
- **Port** – Port number.
- **Name** – Descriptive text (page 3-2).
- **Action** – Indicates the action to be taken when a port security violation is detected:
  - **None**: No action should be taken. (This is the default.)
  - **Trap**: Send an SNMP trap message.

Downloaded from www.Manualslib.com manuals search engine

- **Shutdown**: Disable the port.
- **Trap and Shutdown**: Send an SNMP trap message and disable the port.

- **Status** – Enables or disables port security on the port. (Default: Disabled)
- **Max MAC Count** – The maximum number of MAC addresses that can be learned on a port. (Range: 0 - 20)
- **Trunk** – Trunk number if port is a member (page 3-97 and 3-99).

Web – Click Security, Port Security. Set the action to take when an invalid address is detected on a port, mark the checkbox in the Status column to enable security for a port, set the maximum number of MAC addresses allowed on a port, and click Apply.



Downloaded from www.Manualslib.com manuals search engine

CLI – This example sets the command mode to Port 5, sets the port security action to send a trap and disable the port, and specifies a maximum address count.

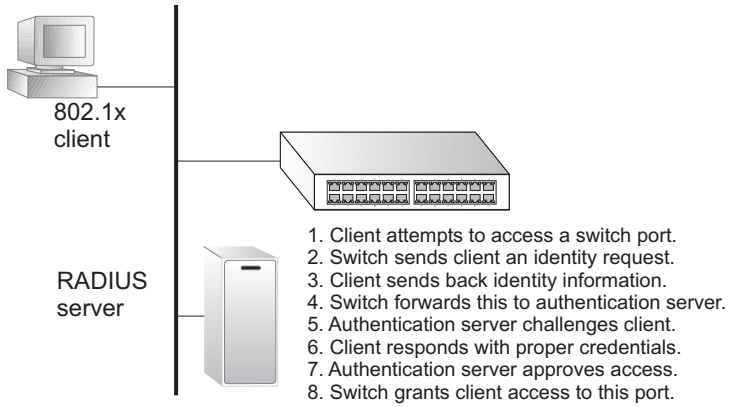
```
Console(config)#interface ethernet 1/5
Console(config-if)#port security action trap-and-shutdown3-101
Console(config-if)#port security max-mac-count 20
Console(config-if)#
```


Downloaded from www.Manualslib.com manuals search engine

Configuring 802.1x Port Authentication

Network switches can provide open and easy access to network resources by simply attaching a client PC. Although this automatic configuration and access is a desirable feature, it also allows unauthorized personnel to easily intrude and possibly gain access to sensitive network data.

The IEEE 802.1x (dot1x) standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. Access to all switch ports in a network can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.


802.1x client
RADIUS server
1. Client attempts to access a switch port.
2. Switch sends client an identity request.
3. Client sends back identity information.
4. Switch forwards this to authentication server.
5. Authentication server challenges client.
6. Client responds with proper credentials.
7. Authentication server approves access.
8. Switch grants client access to this port.

This switch uses the Extensible Authentication Protocol over LANs (EAPOL) to exchange authentication protocol messages with the client, and a remote RADIUS authentication server to verify user identity and access rights. When a client (i.e., Supplicant) connects to a switch port, the switch (i.e., Authenticator) responds with an EAPOL identity request. The client provides its identity (such as a user name) in an EAPOL response to the switch, which it forwards to the RADIUS server. The RADIUS server verifies the client identity and sends an access challenge back to the client. The EAP packet from the RADIUS server contains not only the challenge, but the authentication method to be used. The client can reject the authentication method and request another, depending on the configuration of the client software and the RADIUS server. The authentication method can be MD5, TLS (Transport Layer Security), TTLS (Tunneled Transport Layer Security), or other. The client responds to the appropriate method with its credentials, such as a password or

Downloaded from www.Manualslib.com manuals search engine

certificate. The RADIUS server verifies the client credentials and responds with an accept or reject packet. If authentication is successful, the switch allows the client to access the network. Otherwise, network access is denied and the port remains blocked.

The operation of dot1x on the switch requires the following:

- The switch must have an IP address assigned.
- RADIUS authentication must be enabled on the switch and the IP address of the RADIUS server specified.
- Each switch port that will be used must be set to dot1x "Auto" mode.
- Each client that needs to be authenticated must have dot1x client software installed and properly configured.
- The RADIUS server and 802.1x client support EAP. (The switch only supports EAPOL in order to pass the EAP packets from the server to the client.)
- The RADIUS server and client also have to support the same EAP authentication type – MD5, TLS, TTLS, PEAP, etc. (Some clients have native support in Windows, otherwise the dot1x client must support it.)

Displaying 802.1x Global Settings

The dot1x protocol includes global parameters that control the client authentication process that runs between the client and the switch (i.e., authenticator), as well as the client identity lookup process that runs between the switch and authentication server. These parameters are described in this section.

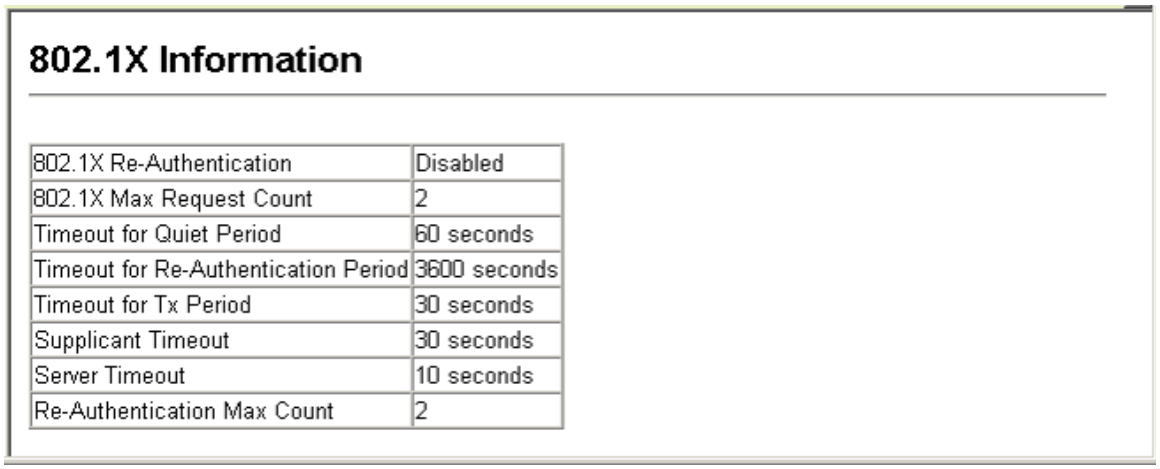
Command Attributes

- **dot1x Re-authentication** – Indicates if switch port requires a client to be re-authenticated after a certain period of time.

Downloaded from www.Manualslib.com manuals search engine

- **dot1x Max Request Count** – The maximum number of times the switch port will retransmit an EAP request packet to the client before it times out the authentication session.
- **Timeout for Quiet Period** – Indicates the time that a switch port waits after the Max Request Count has been exceeded before attempting to acquire a new client.
- **Timeout for Re-authentication Period** – Indicates the time period after which a connected client must be re-authenticated.
- **Timeout for TX Period** – The time period during an authentication session that the switch waits before re-transmitting an EAP packet.
- **Supplicant timeout** – The time the switch waits for a client response to an EAP request.
- **Server timeout** – The time the switch waits for a response from the authentication server (RADIUS) to an authentication request.
- **Re-authentication Max Count** – The number of times the switch will attempt to re-authenticate a connected client before the port becomes unauthorized.

Web – Click 802.1x, Information.


802.1X Information
802.1X Re-Authentication Disabled
802.1X Max Request Count 2
Timeout for Quiet Period 60 seconds
Timeout for Re-Authentication Period 3600 seconds
Timeout for Tx Period 30 seconds
Supplicant Timeout 30 seconds
Server Timeout 10 seconds
Re-Authentication Max Count 2

Downloaded from www.Manualslib.com manuals search engine

CLI – This example shows the default protocol settings for dot1x. For a description of the additional entries displayed in the CLI, see "show dot1x" on page 3-110.

```
Console#show dot1x3-110
Global 802.1X Parameters
 reauth-enabled: yes
 reauth-period:  300
 quiet-period:   350
 tx-period:      300
 supp-timeout:   30
 server-timeout: 30
 reauth-max:     2
 max-req:        2

802.1X Port Summary
 Port Name     Status     Operation Mode                Mode     Authorized
       1/1   disabled        Single-Host      ForceAuthorized            n/a
       1/2   disabled        Single-Host      ForceAuthorized            n/a
.
.
.
      1/23   disabled        Single-Host      ForceAuthorized            yes
      1/24    enabled        Single-Host                Auto            yes

802.1X Port Details

802.1X is disabled on port 1
.
.
.

802.1X is enabled on port 24
Status              Unauthorized
Operation mode      Single-Host
Max count           5
Port-control        Auto
Supplicant          00-00-00-00-00-00
Current Identifier  0

Authenticator State Machine
State               Connecting
Reauth Count        3

Backend State Machine
State               Idle
Request Count       0
Identifier(Server)  0

Reauthentication State Machine
State               Initialize
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Configuring 802.1x Global Settings

The dot1x protocol includes global parameters that control the client authentication process that runs between the client and the switch (i.e., authenticator), as well as the client identity lookup process that runs between the switch and authentication server. The configuration options for these parameters are described in this section.

Command Attributes

- **dot1X Re-authentication** – Sets the client to be re-authenticated after the interval specified by the Timeout for Re-authentication Period. Re-authentication can be used to detect if a new device is plugged into a switch port. (Default: Disabled)

- **dot1X Max Request Count** – Sets the maximum number of times the switch port will retransmit an EAP request packet to the client before it times out the authentication session. (Range: 1-10; Default 2)

- **Timeout for Quiet Period** – Sets the time that a switch port waits after the dot1X Max Request Count has been exceeded before attempting to acquire a new client. (Range: 1-65535 seconds; Default: 60 seconds)

- **Timeout for Re-authentication Period** – Sets the time period after which a connected client must be re-authenticated. (Range: 1-65535 seconds; Default: 3600 seconds)

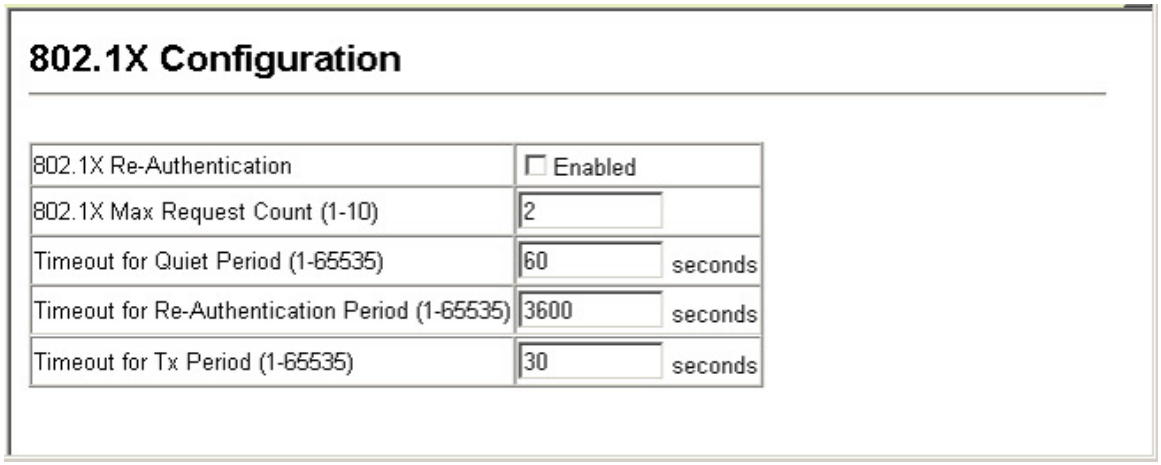
- **Timeout for TX Period** – Sets the time period during an authentication session that the switch waits before re-transmitting an EAP packet. (Range: 1-65535; Default: 30 seconds)

- **authentication dot1x default*** – Sets the default authentication server type. Note that the specified authentication server type must be enabled and properly configured for dot1x to function properly. (Options: radius).

* CLI only.

Downloaded from www.Manualslib.com manuals search engine

Web – Select Security, 802.1x, Configuration. Enable dot1x globally for the switch, modify any of the parameters required, and then click Apply.



CLI – This enables re-authentication and sets all of the global parameters for dot1x.

```
Console(config)#dot1x re-authentication3-108
Console(config)#dot1x max-req 53-105
Console(config)#dot1x timeout quiet-period 403-108
Console(config)#dot1x timeout re-auth 53-109
Console(config)#dot1x timeout tx-period 403-109
Console(config)#authentication dot1x default radius3-105
Console(config)#
```

Configuring Port Authorization Mode

When dot1x is enabled, you need to specify the dot1x authentication mode configured for each port.

Command Attributes

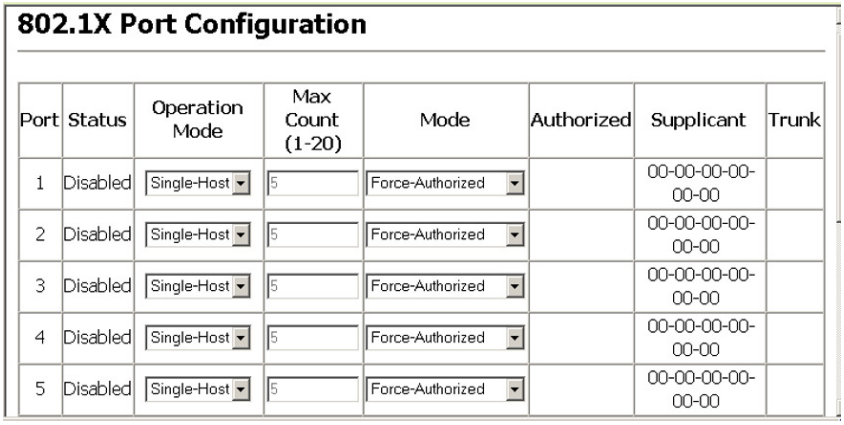
- **Status** – Indicates if authentication is enabled or disabled on the port.
- **Operation Mode** – Allows single or multiple hosts (clients) to connect to an 802.1X-authorized port. (Range: Single-Host, Multi-Host; Default: Single-Host)
- **Max Count** – The maximum number of hosts that can connect to a port when the Multi-Host operation mode is selected. (Range: 1-20;

Downloaded from www.Manualslib.com manuals search engine

Default: 5)

- **Mode** – Sets the authentication mode to one of the following options:
  - **Auto** – Requires a dot1x-aware client to be authorized by the authentication server. Clients that are not dot1x-aware will be denied access.
  - **Force-Authorized** – Forces the port to grant access to all clients, either dot1x-aware or otherwise.
  - **Force-Unauthorized** – Forces the port to deny access to all clients, either dot1x-aware or otherwise.
- **Authorized** –
  - **Yes** – Connected client is authorized.
  - **No** – Connected client is not authorized.
  - *Blank* – Displays nothing when dot1x is disabled on a port.
- **Supplicant** – Indicates the MAC address of a connected client.
- **Trunk** – Indicates if the port is configured as a trunk port.

Web – Click Security, 802.1x, Port Configuration. Select the authentication mode from the drop-down box and click Apply.



Downloaded from www.Manualslib.com manuals search engine

CLI – This example sets the authentication mode to enable 802.1x on port 2, and allows up to ten clients to connect to this port.

```
Console(config)#interface ethernet 1/23-1
Console(config-if)#dot1x port-control auto3-106
Console(config-if)#dot1x operation-mode multi-host max-count 103-107
Console(config-if)#
```

Displaying 802.1x Statistics

This switch can display statistics for dot1x protocol exchanges for any port.

Statistical Values

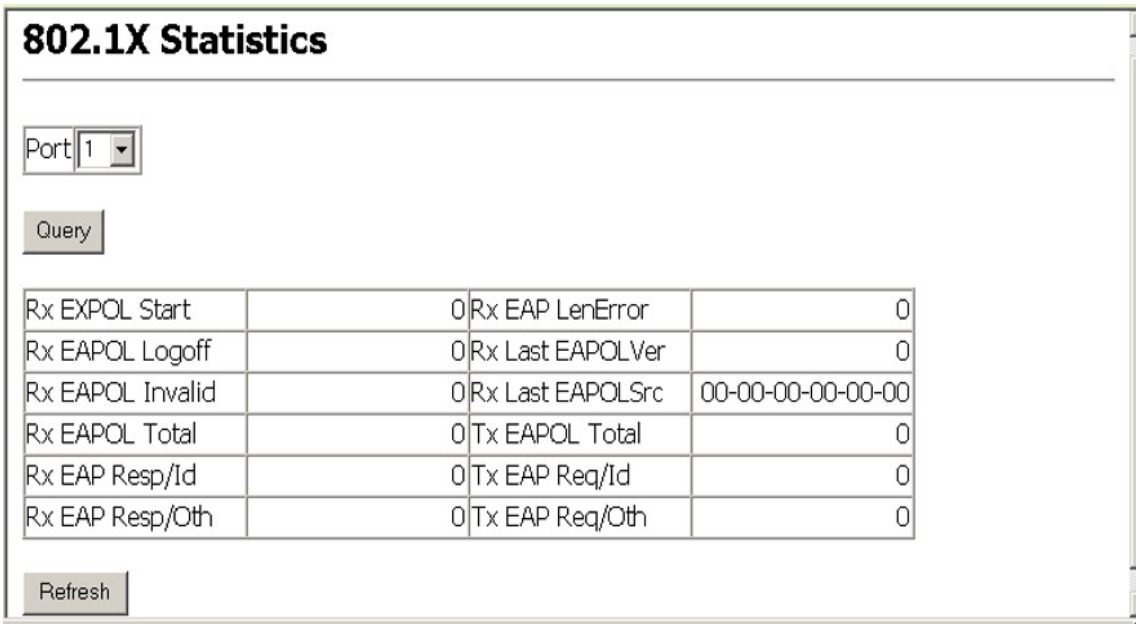
Parameter	Description
Rx EXPOL Start	The number of EAPOL Start frames that have been received by this Authenticator.
Rx EAPOL Logoff	The number of EAPOL Logoff frames that have been received by this Authenticator.
Rx EAPOL Invalid	The number of EAPOL frames that have been received by this Authenticator in which the frame type is not recognized.
Rx EAPOL Total	The number of valid EAPOL frames of any type that have been received by this Authenticator.
Rx EAP Resp/Id	The number of EAP Resp/Id frames that have been received by this Authenticator.
Rx EAP Resp/Oth	The number of valid EAP Response frames (other than Resp/Id frames) that have been received by this Authenticator.
Rx EAP LenError	The number of EAPOL frames that have been received by this Authenticator in which the Packet Body Length field is invalid.
Rx Last EAPOLVer	The protocol version number carried in the most recently received EAPOL frame.
Rx Last EAPOLSrc	The source MAC address carried in the most recently received EAPOL frame.
Tx EAPOL Total	The number of EAPOL frames of any type that have been transmitted by this Authenticator.

Downloaded from www.Manualslib.com manuals search engine

Parameter	Description
Tx EAP Req/Id	The number of EAP Req/Id frames that have been transmitted by this Authenticator.
Tx EAP Req/Oth	The number of EAP Request frames (other than Rq/Id frames) that have been transmitted by this Authenticator.

Downloaded from www.Manualslib.com manuals search engine

Web – Select Security, 802.1x, Statistics. Select the required port and then click Query. Click Refresh to update the statistics.



CLI – This example displays the dot1x statistics for port 4.

```
Console#show dot1x statistics interface ethernet 1/43-110

Eth 1/4
Rx: EXPOL      EAPOL      EAPOL      EAPOL      EAP      EAP      EAP
    Start      Logoff    Invalid     Total    Resp/Id  Resp/Oth LenError
        2           0          0      1007      672         0        0

    Last       Last
EAPOLVer     EAPOLSrc
       1     00-00-E8-98-73-21

Tx: EAPOL      EAP      EAP
    Total     Req/Id   Req/Oth
     2017     1005        0
Console#
```

Filtering Management Access

You can specify the client IP addresses that are allowed management access to the switch through the web interface, SNMP (also see page 3-41), or Telnet.

Downloaded from www.Manualslib.com manuals search engine

Command Usage

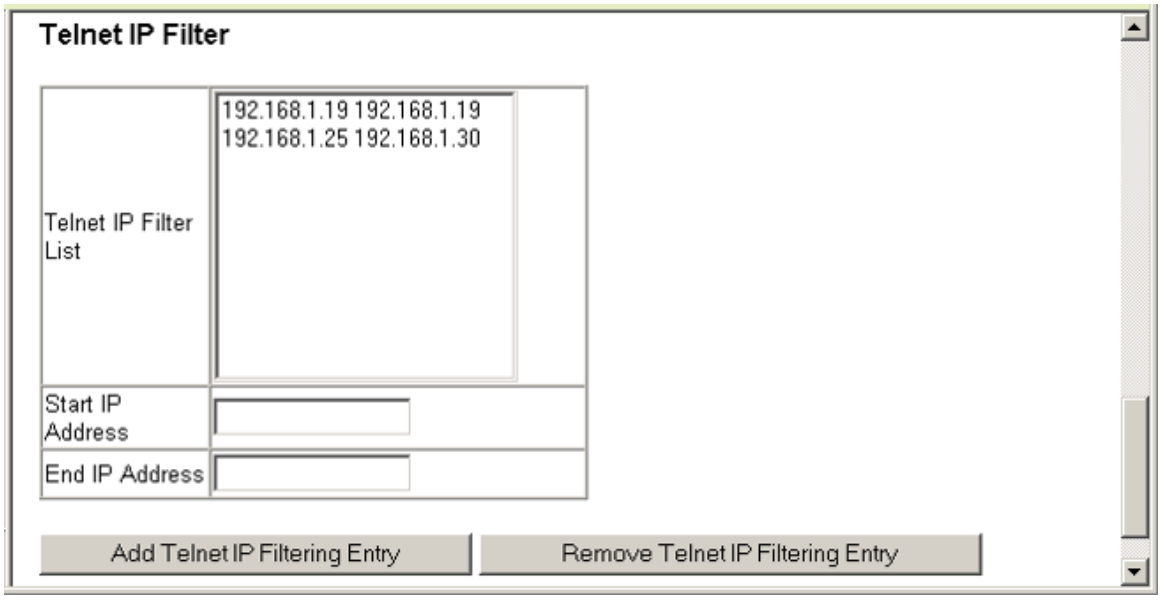
- The management interfaces are open to all IP addresses by default. Once you add an entry to a filter list, access to that interface is restricted to the specified addresses.
- If anyone tries to access a management interface on the switch from an invalid address, the switch will reject the connection, enter an event message in the system log, and send a trap message to the trap manager.
- IP address can be configured for SNMP, web and Telnet access respectively. Each of these groups can include up to five different sets of addresses, either individual addresses or address ranges.
- When entering addresses for the same group (i.e., SNMP, web or Telnet), the switch will not accept overlapping address ranges. When entering addresses for different groups, the switch will accept overlapping address ranges.
- You cannot delete an individual address from a specified range. You must delete the entire range, and reenter the addresses.
- You can delete an address range just by specifying the start address, or by specifying both the start address and end address.

Command Attributes

- **Web IP Filter** – Configures IP address(es) for the web group.
- **SNMP IP Filter** – Configures IP address(es) for the SNMP group.
- **Telnet IP Filter** – Configures IP address(es) for the Telnet group.
- **IP Filter List** – IP address which are allowed management access to this interface.
- **Start IP Address** – A single IP address, or the starting address of a range.
- **End IP Address** – The end address of a range.

Downloaded from www.Manualslib.com manuals search engine

Web – Click Security, IP Filter. Enter the addresses that are allowed management access to an interface, and click Add IP Filtering Entry.



CLI – This example restricts management access for Telnet clients.

```
Console(config)#management telnet-client 192.168.1.193-38
Console(config)#management telnet-client 192.168.1.25 192.168.1.30
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Access Control Lists

Access Control Lists (ACL) provide packet filtering for IP frames (based on address, protocol, Layer 4 protocol port number or TCP control code) or any frames (based on MAC address or Ethernet type). To filter incoming packets, first create an access list, add the required rules, specify a mask to modify the precedence in which the rules are checked, and then bind the list to a specific port.

Configuring Access Control Lists

An ACL is a sequential list of permit or deny conditions that apply to IP addresses, MAC addresses, or other more specific criteria. This switch tests ingress or egress packets against the conditions in an ACL one by one. A packet will be accepted as soon as it matches a permit rule, or dropped as soon as it matches a deny rule. If no rules match for a list of all permit rules, the packet is dropped; and if no rules match for a list of all deny rules, the packet is accepted.

Command Usage

The following restrictions apply to ACLs:

- Each ACL can have up to 32 rules.
- The maximum number of ACLs is also 32.
- However, due to resource restrictions, the average number of rules bound to the ports should not exceed 20.
- You must configure a mask for an ACL rule before you can bind it to a port or set the queue or frame priorities associated with the rule.
- When an ACL is bound to an interface as an egress filter, all entries in the ACL must be deny rules. Otherwise, the bind operation will fail.
- The switch does not support the explicit "deny any any" rule for the egress IP ACL or the egress MAC ACLs. If these rules are included in an ACL, and you attempt to bind the ACL to an interface for egress checking, the bind operation will fail.

The order in which active ACLs are checked is as follows:

Downloaded from www.Manualslib.com manuals search engine

1.User-defined rules in the Egress MAC ACL for egress ports.

2.User-defined rules in the Egress IP ACL for egress ports.

3.User-defined rules in the Ingress MAC ACL for ingress ports.

4.User-defined rules in the Ingress IP ACL for ingress ports.

5.Explicit default rule (permit any any) in the ingress IP ACL for ingress ports.

6.Explicit default rule (permit any any) in the ingress MAC ACL for ingress ports.

7.If no explicit rule is matched, the implicit default is permit all.

Setting the ACL Name and Type

Use the ACL Configuration page to designate the name and type of an ACL.

Command Attributes

- **Name** – Name of the ACL. (Maximum length: 16 characters)

- **Type** – There are three filtering modes:

- Standard: IP ACL mode that filters packets based on the source IP address.
- Extended: IP ACL mode that filters packets based on source or destination IP address, as well as protocol type and protocol port number. If the "TCP" protocol is specified, then you can also filter packets based on the TCP control code.
- MAC: MAC ACL mode that filters packets based on the source or destination MAC address and the Ethernet frame type (RFC 1060).

Web – Click Security, ACL, Configuration. Enter an ACL name in the Name field, select the list type (IP Standard, IP Extended, or MAC), and click Add to open the configuration page for the new list.

Downloaded from www.Manualslib.com manuals search engine

CLI – This example creates a standard IP ACL named bill.

```
Console(config)#access-list ip standard bill3-116
Console(config-std-acl)#
```

Configuring a Standard IP ACL

Command Attributes

- **Action** – An ACL can contain all permit rules or all deny rules. (Default: Permit rules)

- **IP** – Specifies the source IP address. Use "Any" to include all possible addresses, "Host" to specify a specific host address in the Address field, or "IP" to specify a range of addresses with the Address and SubMask fields. (Options: Any, Host, IP; Default: Any)

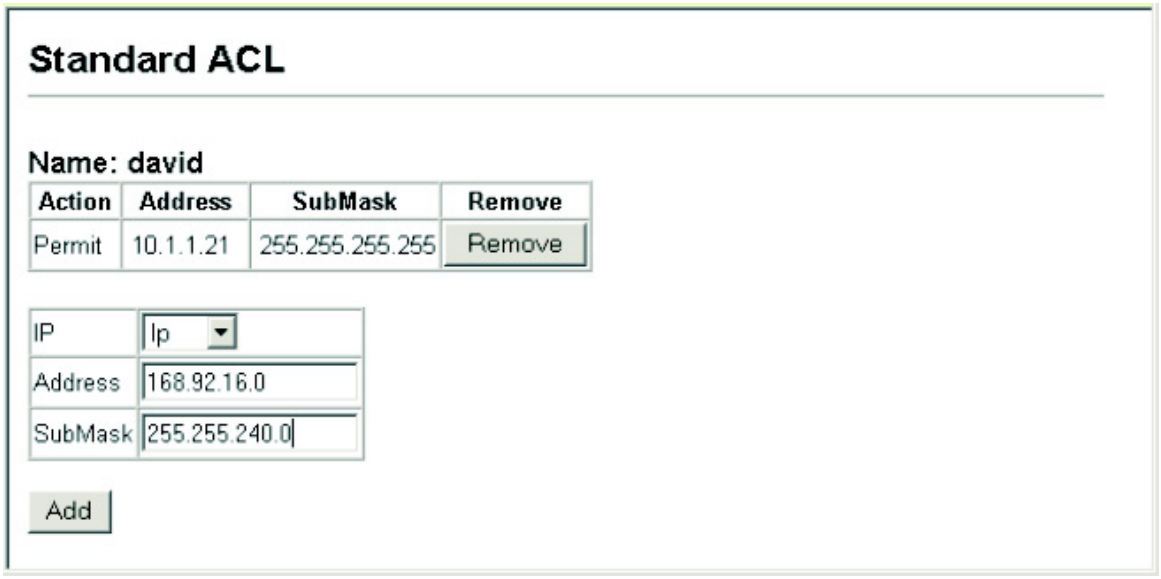
- **Address** – Source IP address.

- **SubMask** – A subnet mask containing four integers from 0 to 255, each separated by a period. The mask uses 1 bits to indicate "match" and 0 bits to indicate "ignore." The mask is bitwise ANDed with the specified source IP address, and compared with the address for each IP packet entering the port(s) to which this ACL has been assigned.

Web – Specify the action (i.e., Permit or Deny). Select the address type (Any, Host, or IP). If you select "Host," enter a specific address. If you

Downloaded from www.Manualslib.com manuals search engine

select "IP," enter a subnet address and the mask for an address range. Then click Add.



CLI – This example configures one permit rule for the specific address 10.1.1.21 and another rule for the address range 168.92.16.x – 168.92.31.x using a bitmask.

```
Console(config-std-acl)#permit host 10.1.1.213-117
Console(config-std-acl)#permit 168.92.16.0 255.255.240.0
Console(config-std-acl)#
```

Configuring an Extended IP ACL

Command Attributes

- **Action** – An ACL can contain either all permit rules or all deny rules. (Default: Permit rules)

- **Src/Dst IP** – Specifies the source or destination IP address. Use "Any" to include all possible addresses, "Host" to specify a specific host address in the Address field, or "IP" to specify a range of addresses with the Address and SubMask fields. (Options: Any, Host, IP; Default: Any)

- **Src/Dst Address** – Source or destination IP address.

- **Src/Dst SubMask** – Subnet mask for source or destination address.

Downloaded from www.Manualslib.com manuals search engine

(See the description for SubMask on page 3-74.)

- **Service Type** – Packet priority settings based on the following criteria:

- **Precedence** – IP precedence level. (Range: 0-7)
- **TOS** – Type of Service level. (Range: 0-15)
- **DSCP** – DSCP priority level. (Range: 0-64)

- **Protocol** – Specifies the protocol type to match as TCP, UDP or Others, where others indicates a specific protocol number (0-255). (Options: TCP, UDP, Others; Default: TCP)

- **Src/Dst Port** – Source/destination port number for the specified protocol type. (Range: 0-65535)

- **Src/Dst Port Bitmask** – Decimal number representing the port bits to match. (Range: 0-65535)

- **Control Code** – Decimal number (representing a bit string) that specifies flag bits in byte 14 of the TCP header. (Range: 0-63)

- **Control Bitmask** – Decimal number representing the code bits to match.
  The control bitmask is a decimal number (for an equivalent binary bit mask) that is applied to the control code. Enter a decimal number, where the equivalent binary bit "1" means to match a bit and "0" means to ignore a bit. The following bits may be specified:

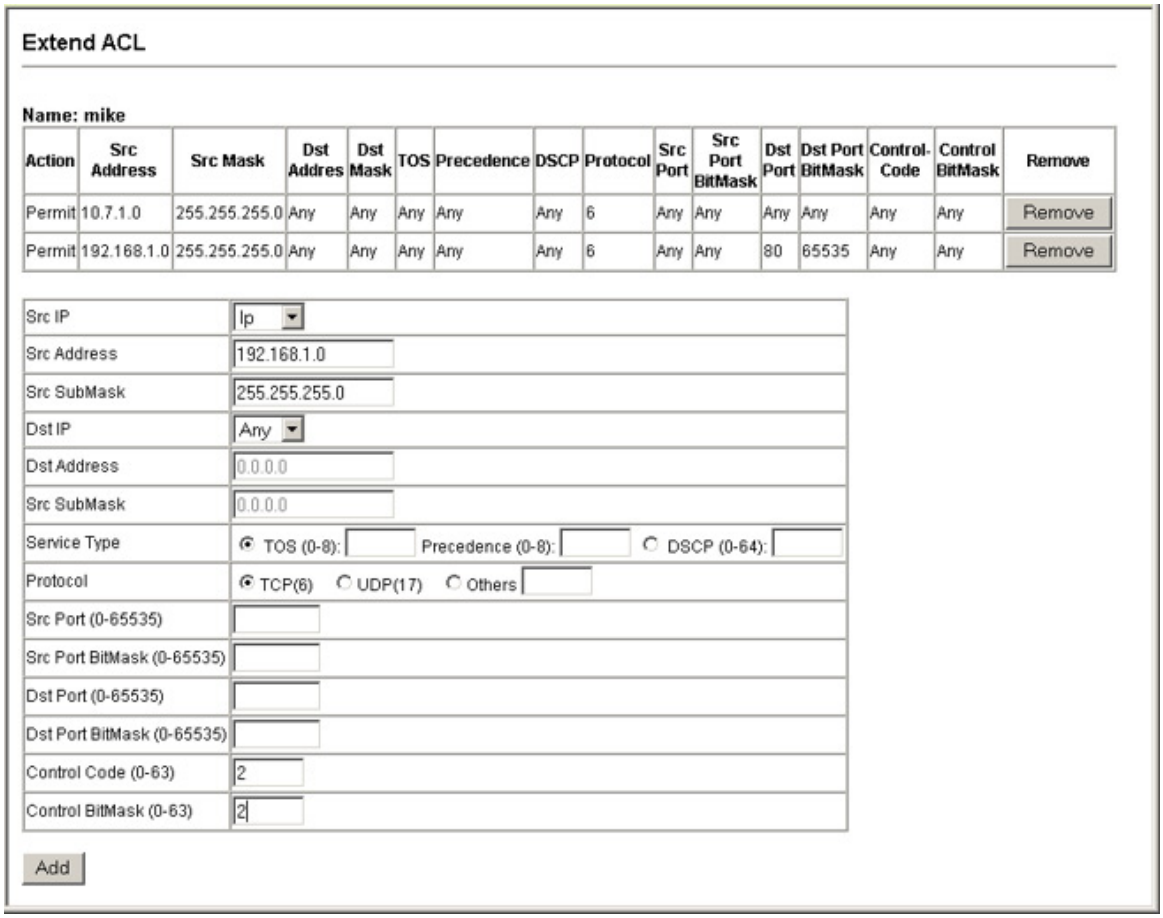
- 1 (fin) – Finish
- 2 (syn) – Synchronize
- 4 (rst) – Reset
- 8 (psh) – Push
- 16 (ack) – Acknowledgement
- 32 (urg) – Urgent pointer

For example, use the code value and mask below to catch packets with the following flags set:

- SYN flag valid, use control-code 2, control bitmask 2
- Both SYN and ACK valid, use control-code 18, control bitmask 18
- SYN valid and ACK invalid, use control-code 2, control bitmask 18

Downloaded from www.Manualslib.com manuals search engine

Web – Specify the action (i.e., Permit or Deny). Specify the source and/or destination addresses. Select the address type (Any, Host, or IP). If you select "Host," enter a specific address. If you select "IP," enter a subnet address and the mask for an address range. Set any other required criteria, such as service type, protocol type, or TCP control code. Then click Add.



CLI – This example adds three rules:

(1)Accept any incoming packets if the source address is in subnet 10.7.1.x. For example, if the rule is matched; i.e., the rule (10.7.1.0 & 255.255.255.0) equals the masked address (10.7.1.2 & 255.255.255.0), the packet passes through.

(2)Allow TCP packets from class C addresses 192.168.1.0 to any destination address when set for destination TCP port 80 (i.e., HTTP).

Downloaded from www.Manualslib.com manuals search engine

(3)Permit all TCP packets from class C addresses 192.168.1.0 with the TCP control code set to "SYN."

```
Console(config-ext-acl)#permit 10.7.1.1 255.255.255.0 any3-118
Console(config-ext-acl)#permit 192.168.1.0 255.255.255.0 any dport 80
Console(config-ext-acl)#permit 192.168.1.0 255.255.255.0 any tcp
control-code 2 2
Console(config-std-acl)#
```

Configuring a MAC ACL

Command Attributes

- **Action** – An ACL can contain all permit rules or all deny rules. (Default: Permit rules)

- **Source/Destination MAC** – Use "Any" to include all possible addresses, "Host" to indicate a specific MAC address, or "MAC" to specify an address range with the Address and Bitmask fields. (Options: Any, Host, MAC; Default: Any)

- **Source/Destination MAC Address** – Source or destination MAC address.

- **Source/Destination MAC Bitmask** – Hexidecimal mask for source or destination MAC address.

- **VID** – VLAN ID. (Range: 1-4095)

- **VID Mask** – VLAN bitmask. (Range: 1-4095)

- **Ethernet Type** – This option can only be used to filter Ethernet II formatted packets. (Range: 600-fff hex.)
  A detailed listing of Ethernet protocol types can be found in RFC 1060. A few of the more common types include 0800 (IP), 0806 (ARP), 8137 (IPX).

- **Ethernet Type Mask** – Protocol bitmask. (Range: 600-fff hex.)

- **Packet Format** – This attribute includes the following packet types:

- **Any** – Any Ethernet packet type.

Downloaded from www.Manualslib.com manuals search engine

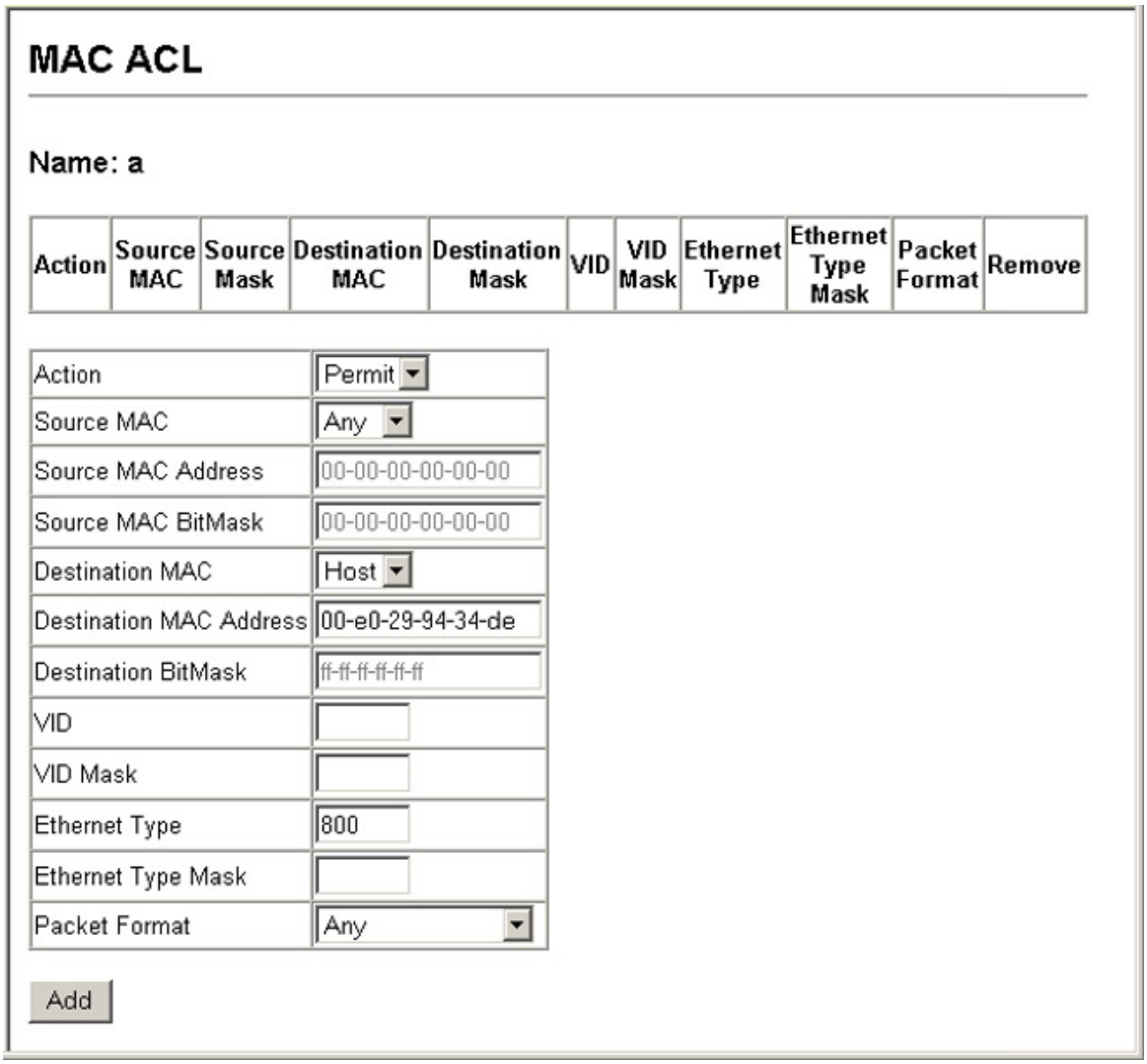
- **Untagged-eth2** – Untagged Ethernet II packets.
- **Untagged-802.3** – Untagged Ethernet 802.3 packets.
- **Tagged-eth2** – Tagged Ethernet II packets.
- **Tagged-802.3** – Tagged Ethernet 802.3 packets.

Command Usage

- Egress MAC ACLs only work for destination-mac-known packets, not for multicast, broadcast, or destination-mac-unknown packets.

Downloaded from www.Manualslib.com manuals search engine

Web – Specify the action (i.e., Permit or Deny). Specify the source and/or destination addresses. Select the address type (Any, Host, or MAC). If you select "Host," enter a specific address (e.g., 11-22-33-44-55-66). If you select "MAC," enter a base address and a hexidecimal bitmask for an address range. Set any other required criteria, such as VID, Ethernet type, or packet format. Then click Add.



CLI – This rule permits packets from any source MAC address to the destination address 00-e0-29-94-34-de where the Ethernet type is 0800.

```
Console(config-mac-acl)#permit any host 00-e0-29-94-34-de ethertype 0800
3-134
Console(config-mac-acl)#
```


Downloaded from www.Manualslib.com manuals search engine

Configuring ACL Masks

You can specify optional masks that control the order in which ACL rules are checked. The switch includes two system default masks that pass/filter packets matching the permit/deny rules specified in an ingress ACL. You can also configure up to seven user-defined masks for an ingress or egress ACL. A mask must be bound exclusively to one of the basic ACL types (i.e., Ingress IP ACL, Egress IP ACL, Ingress MAC ACL or Egress MAC ACL), but a mask can be bound to up to four ACLs of the same type.

Command Usage

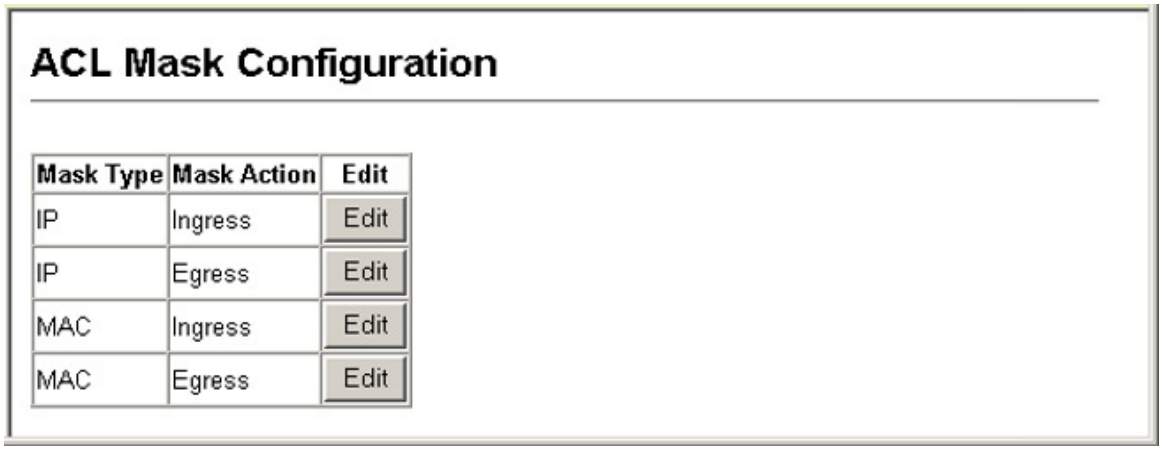
- Up to seven entries can be assigned to an ACL mask.
- Packets crossing a port are checked against all the rules in the ACL until a match is found. The order in which these packets are checked is determined by the mask, and not the order in which the ACL rules are entered.
- First create the required ACLs and the ingress or egress masks before mapping an ACL to an interface.
- You must configure a mask for an ACL rule before you can bind it to a port or set the queue or frame priorities associated with the rule.

Specifying the Mask Type

Use the ACL Mask Configuration page to edit the mask for the Ingress IP ACL, Egress IP ACL, Ingress MAC ACL or Egress MAC ACL.

Downloaded from www.Manualslib.com manuals search engine

Web – Click Security, ACL, ACL Mask Configuration. Click Edit for one of the basic mask types to open the configuration page.



CLI – This example creates an IP ingress mask, and then adds two rules. Each rule is checked in order of precedence to look for a match in the ACL entries. The first entry matching a mask is applied to the inbound packet.

```
Console(config)#access-list ip mask-precedence in3-121
Console(config-ip-mask-acl)#mask host any3-122
Console(config-ip-mask-acl)#mask 255.255.255.0 any
Console(config-ip-mask-acl)#
```

Configuring an IP ACL Mask

This mask defines the fields to check in the IP header.

Command Usage

- Masks that include an entry for a Layer 4 protocol source port or destination port can only be applied to packets with a header length of exactly five bytes.

Command Attributes

- **Src/Dst IP** – Specifies the source or destination IP address. Use "Any" to match any address, "Host" to specify a host address (not a subnet), or "IP" to specify a range of addresses. (Options: Any, Host, IP; Default: Any)

- **Src/Dst IP Bitmask** – Source or destination address of rule must

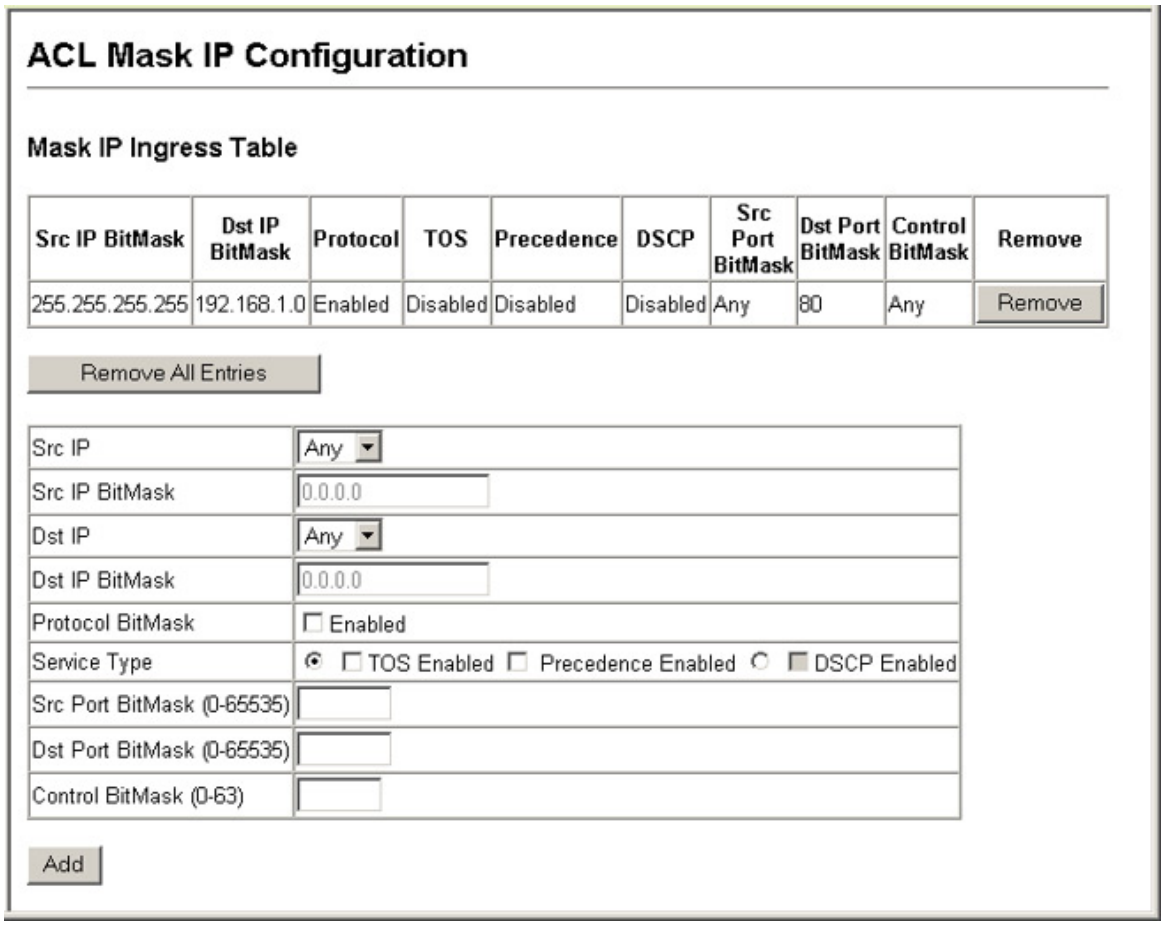
Downloaded from www.Manualslib.com manuals search engine

match this bitmask. (See the description for SubMask on page 3-74.)

- **Protocol Bitmask** – Check the protocol field.
- **Service Type** – Check the rule for the specified priority type. (Options: Precedence, TOS, DSCP; Default: TOS)
- **Src/Dst Port Bitmask** – Protocol port of rule must match this bitmask. (Range: 0-65535)
- **Control Bitmask** – Control flags of rule must match this bitmask. (Range: 0-63)

Downloaded from www.Manualslib.com manuals search engine

Web – Configure the mask to match the required rules in the IP ingress or egress ACLs. Set the mask to check for any source or destination address, a specific host address, or an address range. Include other criteria to search for in the rules, such as a protocol type or one of the service types. Or use a bitmask to search for specific protocol port(s) or TCP control code(s). Then click Add.



CLI – This shows that the entries in the mask override the precedence in which the rules are entered into the ACL. In the following example, packets with the source address 10.1.1.1 are dropped because the "deny

Downloaded from www.Manualslib.com manuals search engine

10.1.1.1 255.255.255.255" rule has the higher precedence according the "mask host any" entry.

```
Console(config)#access-list ip standard A23-116
Console(config-std-acl)#permit 10.1.1.0 255.255.255.03-117
Console(config-std-acl)#deny 10.1.1.1 255.255.255.255
Console(config-std-acl)#exit
Console(config)#access-list ip mask-precedence in3-121
Console(config-ip-mask-acl)#mask host any3-122
Console(config-ip-mask-acl)#mask 255.255.255.0 any
Console(config-ip-mask-acl)#
```

Configuring a MAC ACL Mask

This mask defines the fields to check in the packet header.

Command Usage

You must configure a mask for an ACL rule before you can bind it to a port.

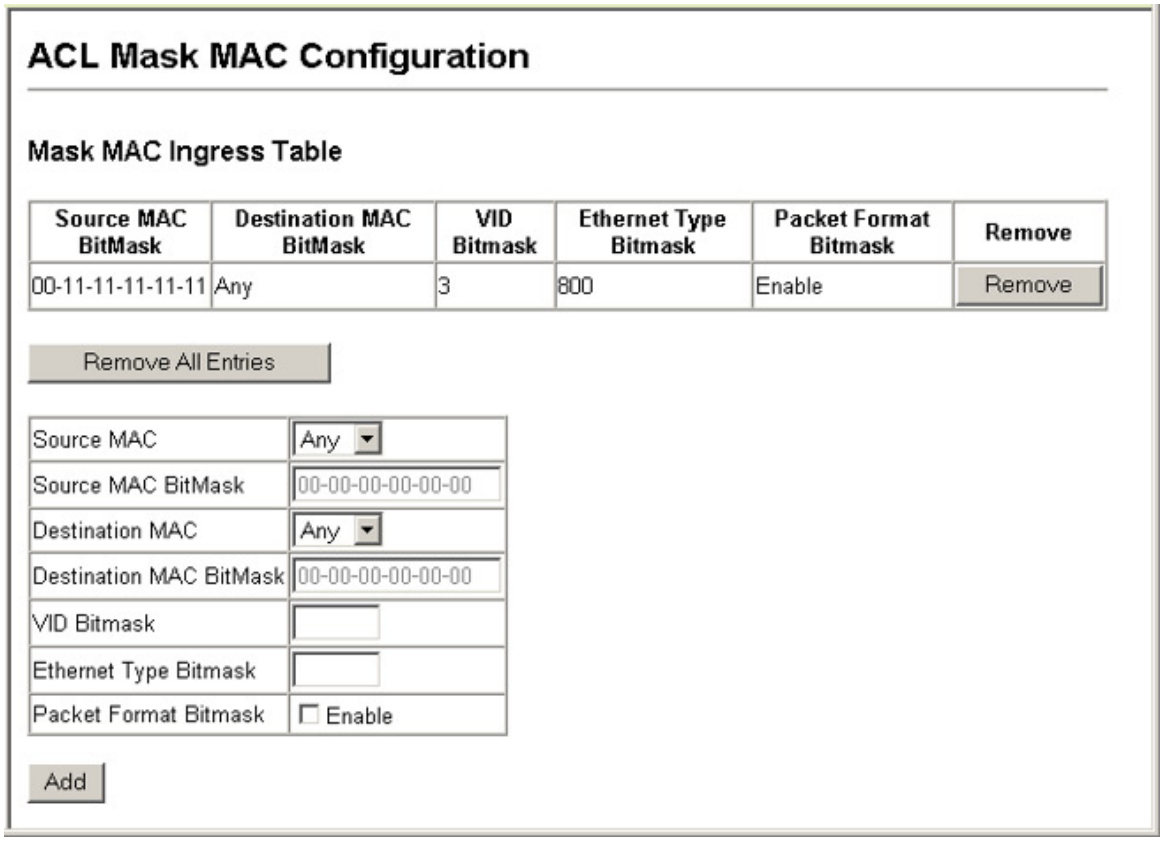
Command Attributes

- **Source/Destination MAC** – Use "Any" to match any address, "Host" to specify the host address for a single node, or "MAC" to specify a range of addresses. (Options: Any, Host, MAC; Default: Any)
- **Source/Destination MAC Bitmask** – Address of rule must match this bitmask.
- **VID Bitmask** – VLAN ID of rule must match this bitmask.
- **Ethernet Type Bitmask** – Ethernet type of rule must match this bitmask.
- **Packet Format Bitmask** – A packet format must be specified in the rule.

Web – Configure the mask to match the required rules in the MAC ingress or egress ACLs. Set the mask to check for any source or destination address, a host address, or an address range. Use a bitmask to search for

Downloaded from www.Manualslib.com manuals search engine

specific VLAN ID(s) or Ethernet type(s). Or check for rules where a packet format was specified. Then click Add.



Downloaded from www.Manualslib.com manuals search engine

CLI – This example shows how to create an Ingress MAC ACL and bind it to a port. You can then see that the order of the rules have been changed by the mask.

```
Console(config)#access-list mac M43-133
Console(config-mac-acl)#permit any any3-134
Console(config-mac-acl)#deny tagged-eth2 00-11-11-11-11-11
ff-ff-ff-ff-ff-ff any vid 33-134
Console(config-mac-acl)#end
Console#show access-list3-146
MAC access-list M4:
  permit any any
  deny tagged-eth2 host 00-11-11-11-11-11 any vid 3
Console(config)#access-list mac mask-precedence in3-137
Console(config-mac-mask-acl)#mask pktformat ff-ff-ff-ff-ff-ff any vid3-138
Console(config-mac-mask-acl)#exit
Console(config)#interface ethernet 1/123-1
Console(config-if)#mac access-group M4 in3-142
Console(config-if)#end
Console#show access-list
MAC access-list M4:
  deny tagged-eth2 host 00-11-11-11-11-11 any vid 3
  permit any any
MAC ingress mask ACL:
  mask pktformat host any vid
Console#
```

Binding a Port to an Access Control List

After configuring the Access Control Lists (ACL), you can bind the ports that need to filter traffic to the appropriate ACLs. You can only bind a port to one ACL for each basic type – IP ingress, IP egress, MAC ingress and MAC egress.

Command Usage

- You must configure a mask for an ACL rule before you can bind it to a port.
- This switch supports ACLs for both ingress and egress filtering. However, you can only bind one IP ACL and one MAC ACL to any port for ingress filtering, and one IP ACL and one MAC ACL to any port for egress filtering. In other words, only four ACLs can be bound to an interface – Ingress IP ACL, Egress IP ACL, Ingress MAC ACL and Egress MAC ACL.
- When an ACL is bound to an interface as an egress filter, all entries in the ACL must be deny rules. Otherwise, the bind operation will fail.

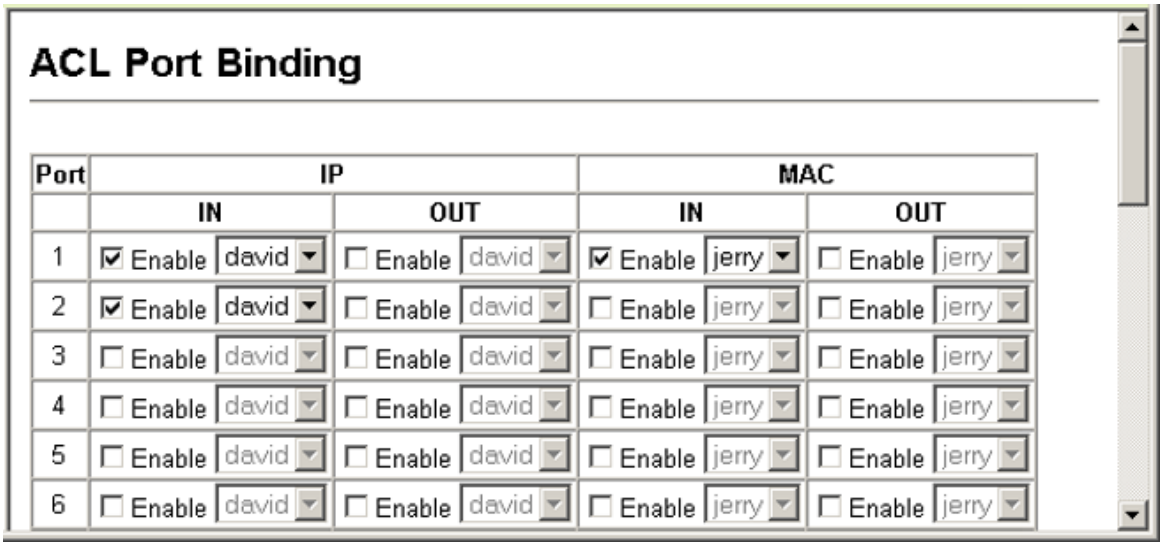
Downloaded from www.Manualslib.com manuals search engine

- The switch does not support the explicit "deny any any" rule for the egress IP ACL or the egress MAC ACLs. If these rules are included in an ACL, and you attempt to bind the ACL to an interface for egress checking, the bind operation will fail.

Command Attributes

- **Port** – Fixed port or SFP module. (Range: 1-12)
- **IP** – Specifies the IP ACL to bind to a port.
- **MAC** – Specifies the MAC ACL to bind to a port.
- **IN** – ACL for ingress packets.
- **OUT** – ACL for egress packets.
- *ACL Name* – Name of the ACL.

Web – Click Security, ACL, Port Binding. Mark the Enable field for the port you want to bind to an ACL for ingress or egress traffic, select the required ACL from the drop-down list, then click Apply.


ACL Port Binding
Port
IP
MAC
IN
OUT
IN
OUT
1 Enable david Enable david Enable jerry Enable jerry
2 Enable david Enable david Enable jerry Enable jerry
3 Enable david Enable david Enable jerry Enable jerry
4 Enable david Enable david Enable jerry Enable jerry
5 Enable david Enable david Enable jerry Enable jerry
6 Enable david Enable david Enable jerry Enable jerry

Downloaded from www.Manualslib.com manuals search engine

CLI – This examples assigns an IP and MAC ingress ACL to port 1, and an IP ingress ACL to port 2.

```
Console(config)#interface ethernet 1/13-1
Console(config-if)#ip access-group david in3-127
Console(config-if)#mac access-group jerry in3-142
Console(config-if)#exit
Console(config)#interface ethernet 1/2
Console(config-if)#ip access-group david in
Console(config-if)#
```

Port Configuration

Displaying Connection Status

You can use the Port Information or Trunk Information pages to display the current connection status, including link state, speed/duplex mode, flow control, and auto-negotiation.

Field Attributes (Web)

- **Name** – Interface label.
- **Type** – Indicates the port type. (1000BASE-T, 1000BASE-SX, 1000BASE-LX)
- **Admin Status** – Shows if the interface is enabled or disabled.
- **Oper Status** – Indicates if the link is Up or Down.
- **Speed Duplex Status** – Shows the current speed and duplex mode. (Auto, or fixed choice)
- **Flow Control Status** – Indicates the type of flow control currently in use.

(IEEE 802.3x, Back-Pressure or None)

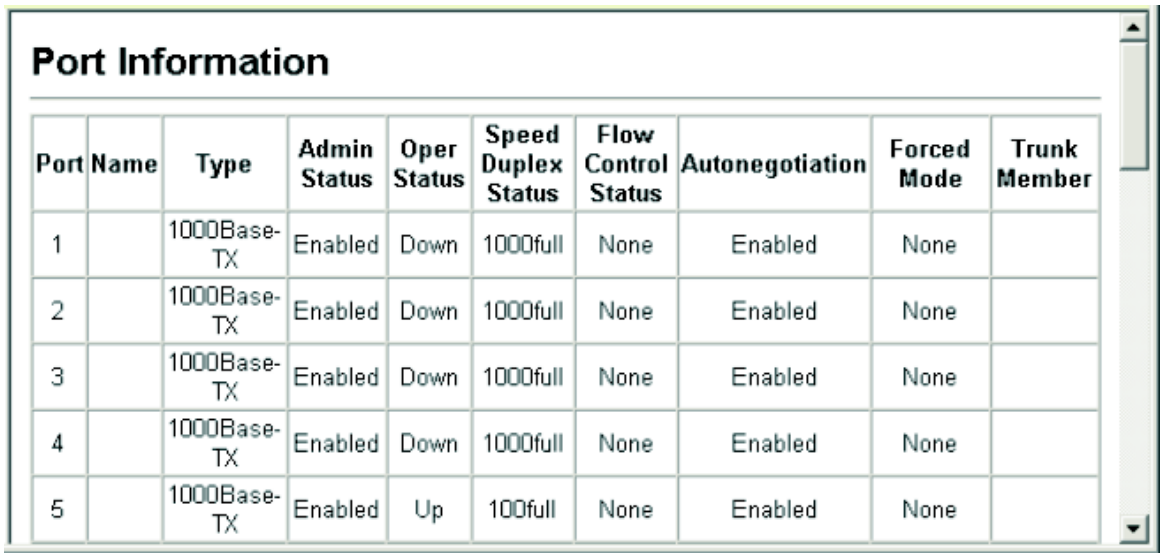
- **Autonegotiation** – Shows if auto-negotiation is enabled or disabled.
- **Forced Mode**[1] – Shows the forced/preferred port type to use for combination ports 9-12. (Copper-Forced, Copper-Preferred-Auto, SFP-Forced, SFP-Preferred-Auto)

Downloaded from www.Manualslib.com manuals search engine

- **Trunk Member**[1] – Shows if port is a trunk member.
- **Creation**[2] – Shows if a trunk is manually configured or dynamically set via LACP.

1: Port Information only.
2: Trunk Information only

Web – Click Port, Port Information or Trunk Information.



Port Information

Port	Name	Type	Admin Status	Oper Status	Speed Duplex Status	Flow Control Status	Autonegotiation	Forced Mode	Trunk Member
1		1000Base-TX	Enabled	Down	1000full	None	Enabled	None	
2		1000Base-TX	Enabled	Down	1000full	None	Enabled	None	
3		1000Base-TX	Enabled	Down	1000full	None	Enabled	None	
4		1000Base-TX	Enabled	Down	1000full	None	Enabled	None	
5		1000Base-TX	Enabled	Up	100full	None	Enabled	None	

Field Attributes (CLI)

Basic information:

- **Port type** – Indicates the port type. (1000BASE-T, 1000BASE-SX, 1000BASE-LX)
- **MAC address** – The physical layer address for this port. (To access this item on the web, see "Setting the Switch's IP Address" on page 3-20.)

Configuration:

- **Name** – Interface label.
- **Port admin** – Shows if the interface is enabled or disabled (i.e., up or down).
- **Speed-duplex** – Shows the current speed and duplex mode. (Auto, or fixed choice)

Downloaded from www.Manualslib.com manuals search engine

- **Capabilities** – Specifies the capabilities to be advertised for a port during auto-negotiation. (To access this item on the web, see "Configuring Interface Connections" on page 3-48.) The following capabilities are supported.
  - **10half** - Supports 10 Mbps half-duplex operation
  - **10full** - Supports 10 Mbps full-duplex operation
  - **100half** - Supports 100 Mbps half-duplex operation
  - **100full** - Supports 100 Mbps full-duplex operation
  - **1000full** - Supports 1000 Mbps full-duplex operation
  - **Sym** - Transmits and receives pause frames for flow control
  - **FC** - Supports flow control
- **Broadcast storm** – Shows if broadcast storm control is enabled or disabled.
- **Broadcast storm limit** – Shows the broadcast storm threshold. (500 - 262143 packets per second)
- **Flow control** – Shows if flow control is enabled or disabled.
- **LACP** – Shows if LACP is enabled or disabled.
- **Port Security** – Shows if port security is enabled or disabled.
- **Max MAC count** – Shows the maximum number of MAC address that can be learned by a port. (0 - 20 addresses)
- **Port security action** – Shows the response to take when a security violation is detected. (shutdown, trap, trap-and-shutdown)
- **Combo forced mode** – Shows the forced/preferred port type to use for combination ports 9-12. (copper forced, copper preferred auto, SFP forced, SFP preferred auto)

Current status:

- **Link Status** – Indicates if the link is up or down.
- **Operation speed-duplex** – Shows the current speed and duplex

Downloaded from www.Manualslib.com manuals search engine

mode.

- **Flow control type** – Indicates the type of flow control currently in use. (IEEE 802.3x, Back-Pressure or none)

CLI – This example shows the connection status for Port 5.

```
Console#show interfaces status ethernet 1/53-11
Information of Eth 1/13
 Basic information:
  Port type: 1000T
  Mac address: 00-30-f1-47-58-46
 Configuration:
  Name:
  Port admin: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full, 1000full,
  Broadcast storm: Enabled
  Broadcast storm limit: 500 packets/second
  Flow control: Disabled
  Lacp: Disabled
  Port security: Disabled
  Max MAC count: 0
  Port security action: None
  Combo forced mode: None
 Current status:
  Link status: Down
  Operation speed-duplex: 100full
  Flow control type: None
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Configuring Interface Connections

You can use the Port Configuration or Trunk Configuration page to enable/disable an interface, set auto-negotiation and the interface capabilities to advertise, or manually fix the speed, duplex mode, and flow control.

Command Attributes

- **Name** – Allows you to label an interface. (Range: 1-64 characters)
- **Admin** – Allows you to manually disable an interface. You can disable an interface due to abnormal behavior (e.g., excessive collisions), and then reenable it after the problem has been resolved. You may also disable an interface for security reasons.
- **Speed/Duplex** – Allows you to manually set the port speed and duplex mode.
- **Flow Control** – Allows automatic or manual selection of flow control.
- **Autonegotiation** (Port Capabilities) – Allows auto-negotiation to be enabled/disabled. When auto-negotiation is enabled, you need to specify the capabilities to be advertised. When auto-negotiation is disabled, you can force the settings for speed, mode, and flow control.The following capabilities are supported.
  - **10half** - Supports 10 Mbps half-duplex operation
  - **10full** - Supports 10 Mbps full-duplex operation
  - **100half** - Supports 100 Mbps half-duplex operation
  - **100full** - Supports 100 Mbps full-duplex operation
  - **1000full** - Supports 1000 Mbps full-duplex operation
  - **Sym** (Gigabit only) - Check this item to transmit and receive pause frames, or clear it to auto-negotiate the sender and receiver for asymmetric pause frames. (*The current switch chip only supports symmetric pause frames.*)
  - **FC** - Supports flow control
    Flow control can eliminate frame loss by "blocking" traffic from end

Downloaded from www.Manualslib.com manuals search engine

stations or segments connected directly to the switch when its buffers fill. When enabled, back pressure is used for half-duplex operation and IEEE 802.3x for full-duplex operation. (Avoid using flow control on a port connected to a hub unless it is actually required to solve a problem. Otherwise back pressure jamming signals may degrade overall performance for the segment attached to the hub.)

(Default: Autonegotiation enabled; Advertised capabilities for 1000BASE-T – 10half, 10full, 100half, 100full, 1000full; 1000BASE-SX/LX/LH – 1000full)

- **Forced Mode** – Shows the forced/preferred port type to use for the combination ports 9-12.

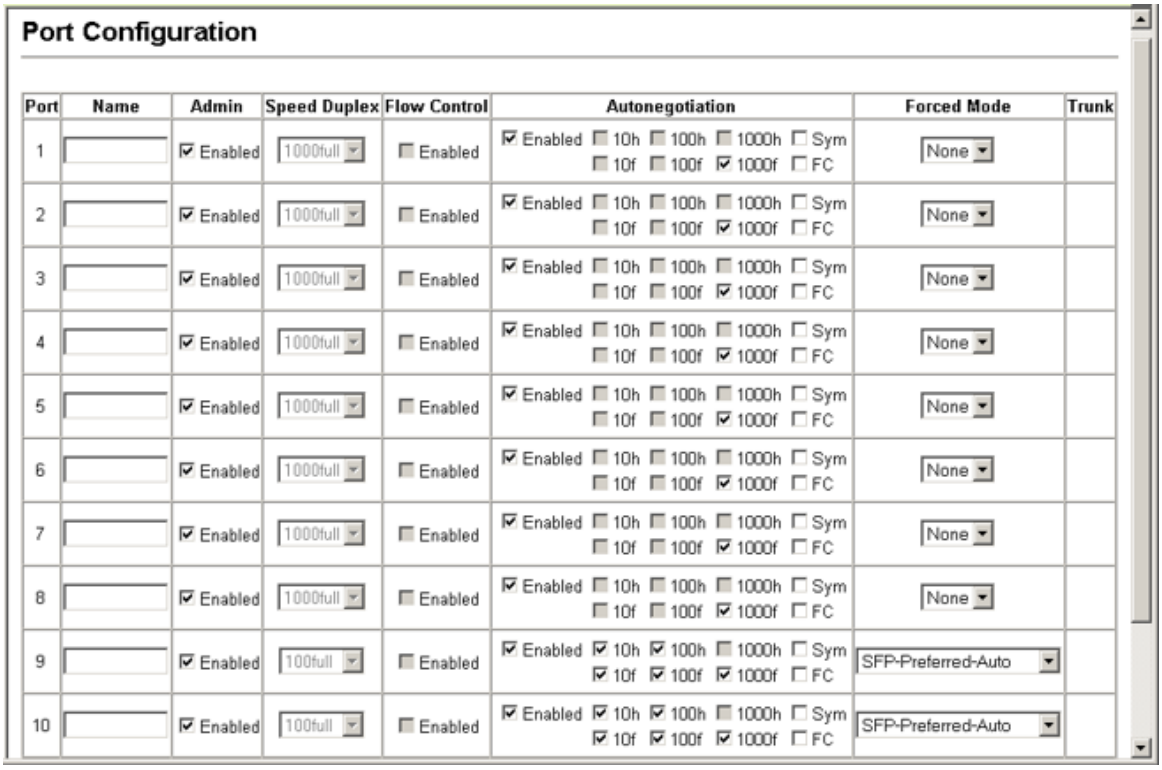
  - **Copper-Forced** - Always uses the built-in RJ-45 port.
  - **Copper-Preferred-Auto** - Uses the built-in RJ-45 port if both combination types are functioning and the RJ-45 port has a valid link.
  - **SFP-Forced** - Always uses the SFP port (even if module is not installed).
  - **SFP-Preferred-Auto** - Uses SFP port if both combination types are functioning and the SFP port has a valid link.

- **Trunk** – Indicates if a port is a member of a trunk. To create trunks and select port members, see "Creating Trunk Groups" on page 3-96.

Note: Auto-negotiation must be disabled before you can configure or force the interface to use the Speed/Duplex Mode or Flow Control options.

Downloaded from www.Manualslib.com manuals search engine

Web – Click Port, Port Configuration or Trunk Configuration. Modify the required interface settings, and click Apply.



Port Configuration

Port	Name	Admin	Speed Duplex	Flow Control	Autonegotiation	Forced Mode	Trunk
1		Enabled	1000full	Enabled	Enabled 10h 100h 1000h Sym 10f 100f 1000f FC	None	
2		Enabled	1000full	Enabled	Enabled 10h 100h 1000h Sym 10f 100f 1000f FC	None	
3		Enabled	1000full	Enabled	Enabled 10h 100h 1000h Sym 10f 100f 1000f FC	None	
4		Enabled	1000full	Enabled	Enabled 10h 100h 1000h Sym 10f 100f 1000f FC	None	
5		Enabled	1000full	Enabled	Enabled 10h 100h 1000h Sym 10f 100f 1000f FC	None	
6		Enabled	1000full	Enabled	Enabled 10h 100h 1000h Sym 10f 100f 1000f FC	None	
7		Enabled	1000full	Enabled	Enabled 10h 100h 1000h Sym 10f 100f 1000f FC	None	
8		Enabled	1000full	Enabled	Enabled 10h 100h 1000h Sym 10f 100f 1000f FC	None	
9		Enabled	100full	Enabled	Enabled 10h 100h 1000h Sym 10f 100f 1000f FC	SFP-Preferred-Auto	
10		Enabled	100full	Enabled	Enabled 10h 100h 1000h Sym 10f 100f 1000f FC	SFP-Preferred-Auto	

CLI – Select the interface, and then enter the required settings.

```
Console(config)#interface ethernet 1/13 3-1
Console(config-if)#description RD SW#13 3-2
Console(config-if)#shutdown 3-9
.
Console(config-if)#no shutdown
Console(config-if)#no negotiation 3-4
Console(config-if)#speed-duplex 100half 3-3
Console(config-if)#flowcontrol 3-7
.
Console(config-if)#negotiation
Console(config-if)#capabilities 100half 3-5
Console(config-if)#capabilities 100full
Console(config-if)#capabilities flowcontrol
Console(config-if)#exit
Console(config)#interface ethernet 1/21
Console(config-if)#combo-forced-mode copper-forced 3-8
Console(config-if)#
```


Downloaded from www.Manualslib.com manuals search engine

Creating Trunk Groups

You can create multiple links between devices that work as one virtual, aggregate link. A port trunk offers a dramatic increase in bandwidth for network segments where bottlenecks exist, as well as providing a fault-tolerant link between two devices. You can create up to six trunks at a time.

The switch supports both static trunking and dynamic Link Aggregation Control Protocol (LACP). Static trunks have to be manually configured at both ends of the link, and the switches must comply with the Cisco EtherChannel standard. On the other hand, LACP configured ports can automatically negotiate a trunked link with LACP-configured ports on another device. You can configure any number of ports on the switch as LACP, as long as they are not already configured as part of a static trunk. If ports on another device are also configured as LACP, the switch and the other device will negotiate a trunk link between them. If an LACP trunk consists of more than four ports, all other ports will be placed in a standby mode. Should one link in the trunk fail, one of the standby ports will automatically be activated to replace it.

Command Usage

Besides balancing the load across each port in the trunk, the other ports provide redundancy by taking over the load if a port in the trunk fails. However, before making any physical connections between devices, use the web interface or CLI to specify the trunk on the devices at both ends. When using a port trunk, take note of the following points:

- Finish configuring port trunks before you connect the corresponding network cables between switches to avoid creating a loop.
- You can create up to six trunks on the switch, with up to eight ports per trunk.
- The ports at both ends of a connection must be configured as trunk ports.

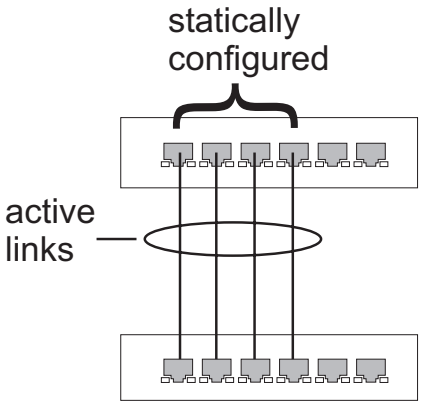
Downloaded from www.Manualslib.com manuals search engine

- When configuring static trunks on switches of different types, they must be compatible with the Cisco EtherChannel standard.
- The ports at both ends of a trunk must be configured in an identical manner, including communication mode (i.e., speed, duplex mode and flow control), VLAN assignments, and CoS settings.
- All the ports in a trunk have to be treated as a whole when moved from/to, added or deleted from a VLAN.
- STP, VLAN, and IGMP settings can only be made for the entire trunk.

Statically Configuring a Trunk

Command Usage

- When configuring static trunks, you may not be able to link switches of different types, depending on the manufacturer's implementation. However, note that the static trunks on this switch are Cisco EtherChannel compatible.

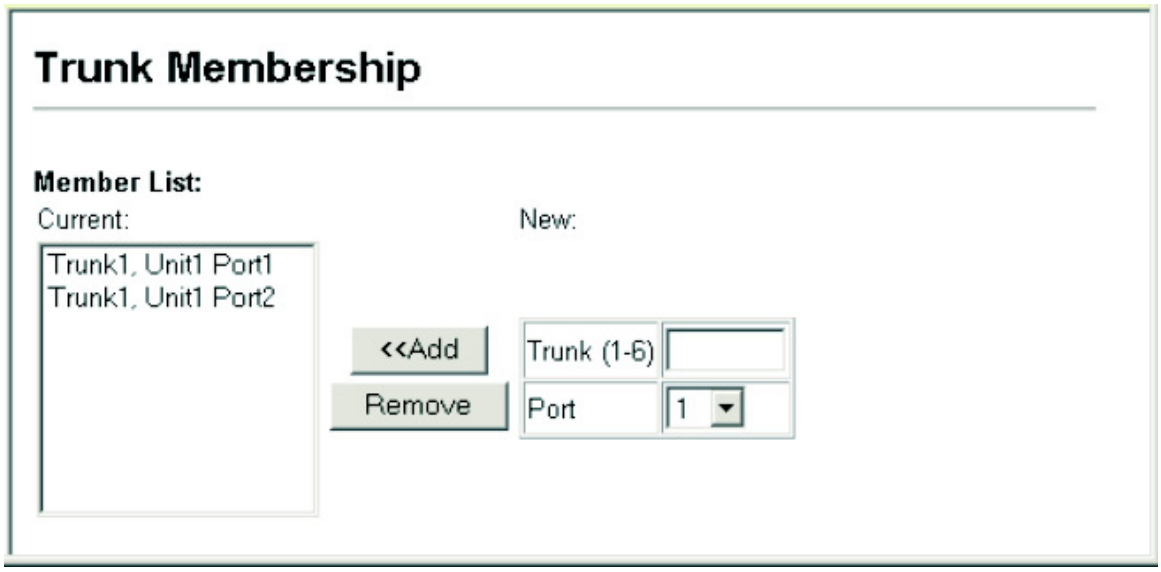


- To avoid creating a loop in the network, be sure you add a static trunk via the configuration interface before connecting the ports, and also disconnect the ports before removing a static trunk via the configuration interface.

Web – Click Trunk, Trunk Membership. Enter a trunk ID of 1-6 in the Trunk field, select any of the switch ports from the scroll-down port list,

Downloaded from www.Manualslib.com manuals search engine

and click Add. After you have completed adding ports to the member list, click Apply.



Downloaded from www.Manualslib.com manuals search engine

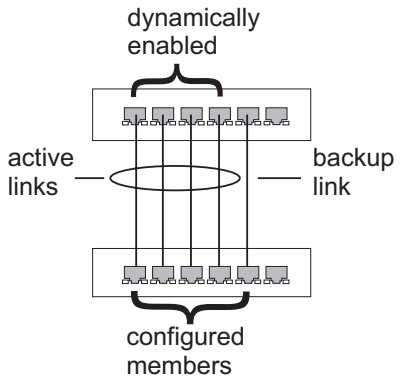
CLI – This example creates trunk 2 with ports 9 and 10. Just connect these ports to two static trunk ports on another switch to form a trunk.

```
Console(config)#interface port-channel 23-1
Console(config-if)#exit
Console(config)#interface ethernet 1/93-1
Console(config-if)#channel-group 13-21
Console(config-if)#exit
Console(config)#interface ethernet 1/10
Console(config-if)#channel-group 1
Console(config-if)#end
Console#show interfaces status port-channel 13-11
Information of Trunk 1
 Basic information:
  Port type: 1000T
  Mac address: 00-00-E8-AA-AA-01
 Configuration:
  Name:
  Port admin: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full, 1000full,
  Flow control: Disabled
  Port security: Disabled
  Max MAC count: 0
  Port security action: None
  Combo forced mode: None
 Current status:
  Created by: User
  Link status: Down
  Operation speed-duplex: 1000full
  Flow control type: None
  Member Ports: Eth1/9, Eth1/10,
Console#
```

Enabling LACP on Selected Ports

Command Usage

- To avoid creating a loop in the network, be sure you enable LACP before connecting the ports, and also disconnect the ports before disabling LACP.



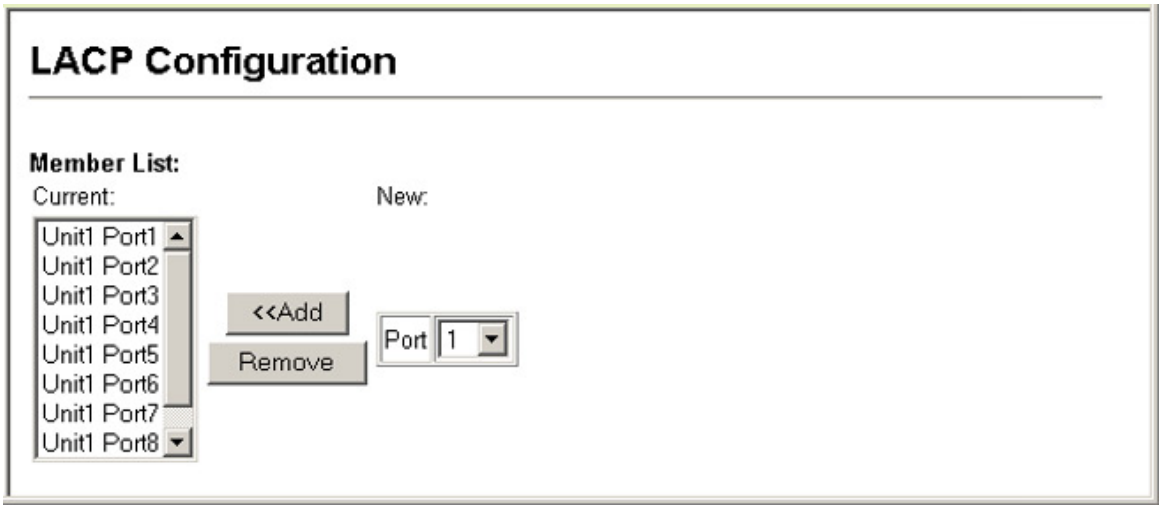
- If the target switch has also enabled LACP on the connected ports, the trunk will be activated automatically.
- A trunk formed with another switch using LACP will automatically be

Downloaded from www.Manualslib.com manuals search engine

assigned the next available trunk ID.

- If more than four ports attached to the same target switch have LACP enabled, the additional ports will be placed in standby mode, and will only be enabled if one of the active links fails.
- All ports on both ends of an LACP trunk must be configured for full duplex, either by forced mode or auto-negotiation.

Web – Click Port, LACP, Configuration. Select any of the switch ports from the scroll-down port list and click Add. After you have completed adding ports to the member list, click Apply.



Downloaded from www.Manualslib.com manuals search engine

CLI – The following example enables LACP for ports 1 to 6. Just connect these ports to LACP-enabled trunk ports on another switch to form a trunk.

```
Console(config)#interface ethernet 1/13-1
Console(config-if)#lacp3-22
Console(config-if)#exit
.
.
.
Console(config)#interface ethernet 1/6
Console(config-if)#lacp
Console(config-if)#end
Console#show interfaces status port-channel 13-11
Information of Trunk 1
 Basic information:
  Port type: 1000T
  Mac address: 22-22-22-22-22-2d
 Configuration:
  Name:
  Port admin status: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full, 1000full,
  Flow control status: Disabled
  Port security: Disabled
  Max MAC count: 0
  Port security action: None
  Combo forced mode: None
 Current status:
  Created by: Lacp
  Link status: Up
  Port operation status: Up
  Operation speed-duplex: 1000full
  Flow control type: None
  Member Ports: Eth1/1, Eth1/2, Eth1/3, Eth1/4, Eth1/5, Eth1/6,
Console#
```

Configuring LACP Parameters

Dynamically Creating a Port Channel –

Ports assigned to a common port channel must meet the following criteria:

- Ports must have the same LACP System Priority.
- Ports must have the same LACP port Admin Key.
- However, if the "port channel" Admin Key is set (page 4-142), then the port Admin Key must be set to the same value for a port to be allowed to join a channel group.

Downloaded from www.Manualslib.com manuals search engine

Note – If the port channel admin key (lacp admin key, page 3-26) is not set (through the CLI) when a channel group is formed (i.e., it has a null value of 0), this key is set to the same value as the port admin key used by the interfaces that joined the group (lacp admin key, as described in this section and on page 3-25).

Command Attributes

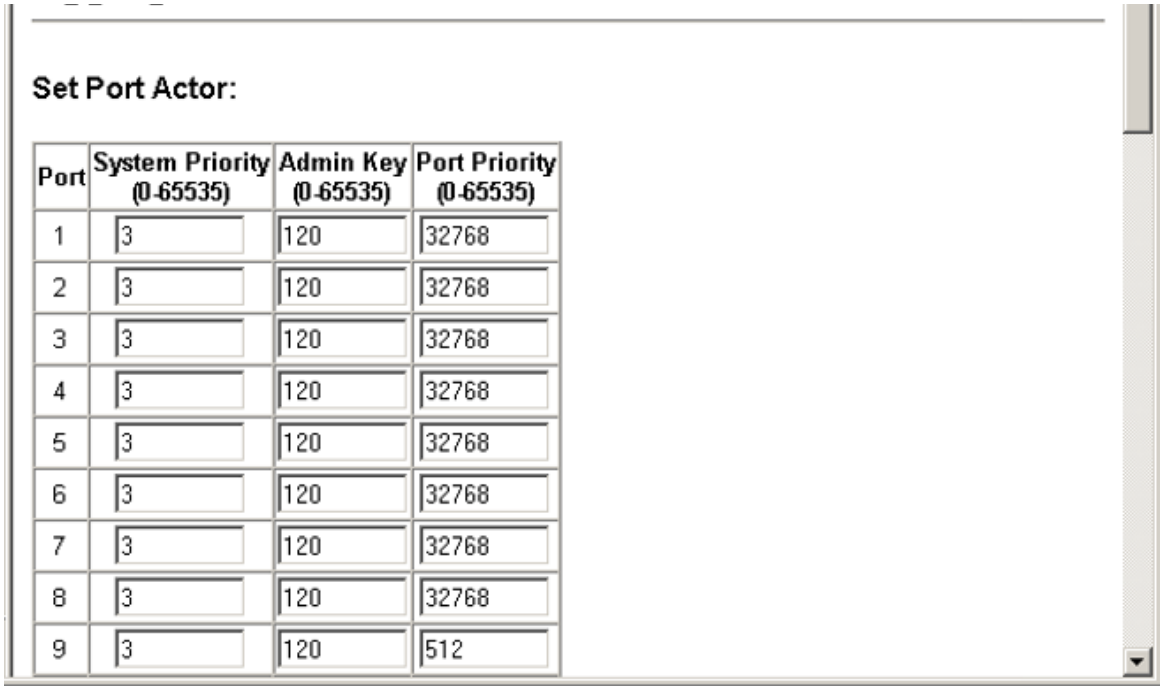
Set Port Actor – This menu sets the local side of an aggregate link; i.e., the ports on this switch.

- **Port** – Port number. (Range: 1-12)
- **System Priority** – LACP system priority is used to determine link aggregation group (LAG) membership, and to identify this device to other switches during LAG negotiations. (Range: 0-65535; Default: 32768)
  - Ports must be configured with the same system priority to join the same LAG.
  - System priority is combined with the switch's MAC address to form the LAG identifier. This identifier is used to indicate a specific LAG during LACP negotiations with other systems.
- **Admin Key** – The LACP administration key must be set to the same value for ports that belong to the same LAG. (Range: 0-65535; Default: 0)
- **Port Priority** – If a link goes down, LACP port priority is used to select a backup link. (Range: 0-65535; Default: 32768)

Set Port Partner – This menu sets the remote side of an aggregate link; i.e., the ports on the attached device. The command attributes have the same meaning as those used for the port actor. However, configuring LACP settings for the partner only applies to its administrative state, not its operational state, and will only take effect the next time an aggregate link is established with the partner.

Downloaded from www.Manualslib.com manuals search engine

Web – Click Port, LACP, Aggregation Port. Set the System Priority, Admin Key, and Port Priority for the Port Actor. You can optionally configure these settings for the Port Partner. (Be aware that these settings only affect the administrative state of the partner, and will not take effect until the next time an aggregate link is formed with this device.) After you have completed setting the port LACP parameters, click Apply.



Set Port Actor:

Port	System Priority (0-65535)	Admin Key (0-65535)	Port Priority (0-65535)
1	3	120	32768
2	3	120	32768
3	3	120	32768
4	3	120	32768
5	3	120	32768
6	3	120	32768
7	3	120	32768
8	3	120	32768
9	3	120	512

Downloaded from www.Manualslib.com manuals search engine

CLI – The following example configures LACP parameters for ports 1-6. Ports 1-4 are used as active members of the LAG; ports 5 and 6 are set to backup mode.

```
Console(config)#interface ethernet 1/13-1
Console(config-if)#lacp actor system-priority 33-24
Console(config-if)#lacp actor admin-key 1203-25
Console(config-if)#lacp actor port-priority 1283-27
Console(config-if)#exit
.
.
.
Console(config)#interface ethernet 1/6
Console(config-if)#lacp actor system-priority 3
Console(config-if)#lacp actor admin-key 120
Console(config-if)#lacp actor port-priority 512
Console(config-if)#end
Console#show lacp sysid3-28
Channel Group    System Priority    System MAC Address
-------------------------------------------------------------------------------
            1              32768     00-00-E9-31-31-31
            2              32768     00-00-E9-31-31-31
            3              32768     00-00-E9-31-31-31
            4              32768     00-00-E9-31-31-31
            5              32768     00-00-E9-31-31-31
            6              32768     00-00-E9-31-31-31
Console#show lacp 1 internal3-28
Channel group : 1
-------------------------------------------------------------------------------
Oper Key : 120
Admin Key : 120
Console#
```

Displaying LACP Port Counters

You can display statistics for LACP protocol messages.

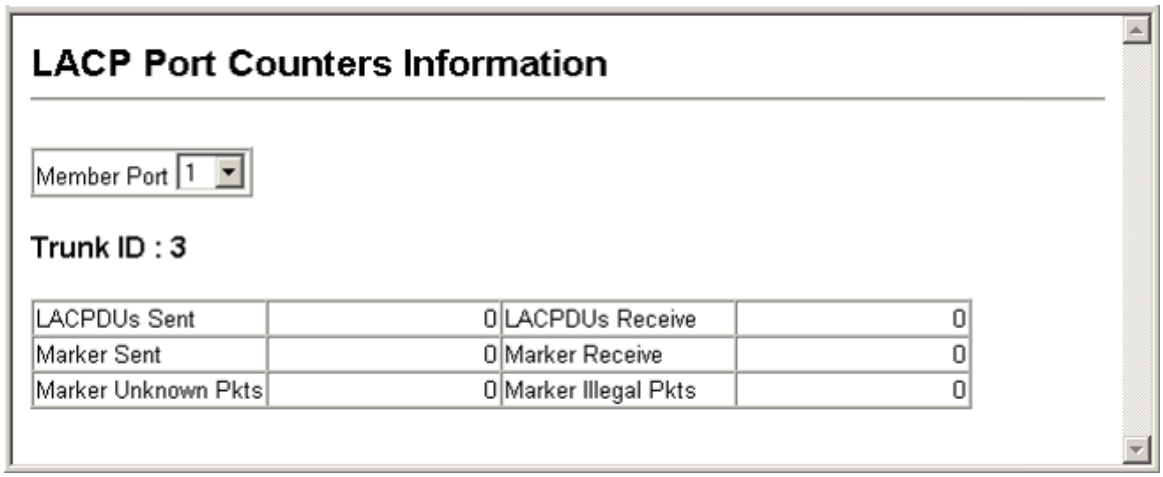
Counter Information

Parameter	Description
LACPDUs Sent	Number of valid LACPDUs transmitted from this channel group.
LACPDUs Received	Number of valid LACPDUs received by this channel group.
Marker Sent	Number of valid Marker PDUs transmitted from this channel group.
Marker Received	Number of valid Marker PDUs received by this channel group.

Downloaded from www.Manualslib.com manuals search engine

Parameter	Description
LACPDUs Unknown Pkts	Number of frames received that either (1) Carry the Slow Protocols Ethernet Type value, but contain an unknown PDU, or (2) are addressed to the Slow Protocols group MAC Address, but do not carry the Slow Protocols Ethernet Type.
LACPDUs Illegal Pkts	Number of frames that carry the Slow Protocols Ethernet Type value, but contain a badly formed PDU or an illegal value of Protocol Subtype.

Web – Click Port, LACP, Port Counters Information. Select a member port to display the corresponding information.


LACP Port Counters Information
Member Port 1
Trunk ID : 3
LACPDUs Sent 0 LACPDUs Receive 0
Marker Sent 0 Marker Receive 0
Marker Unknown Pkts 0 Marker Illegal Pkts 0

CLI – The following example displays LACP counters for port channel 1.

```
Console#show 1 lacp counters3-28
Channel group : 1
-------------------------------------------------------------------------
Eth 1/ 1
-------------------------------------------------------------------------
  LACPDUs Sent : 21
  LACPDUs Received : 21
  Marker Sent : 0
  Marker Received : 0
  LACPDUs Unknown Pkts : 0
  LACPDUs Illegal Pkts : 0
.
.
.
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Displaying LACP Settings and Status for the Local Side

You can display configuration settings and the operational state for the local side of an link aggregation.

Internal Configuration Information

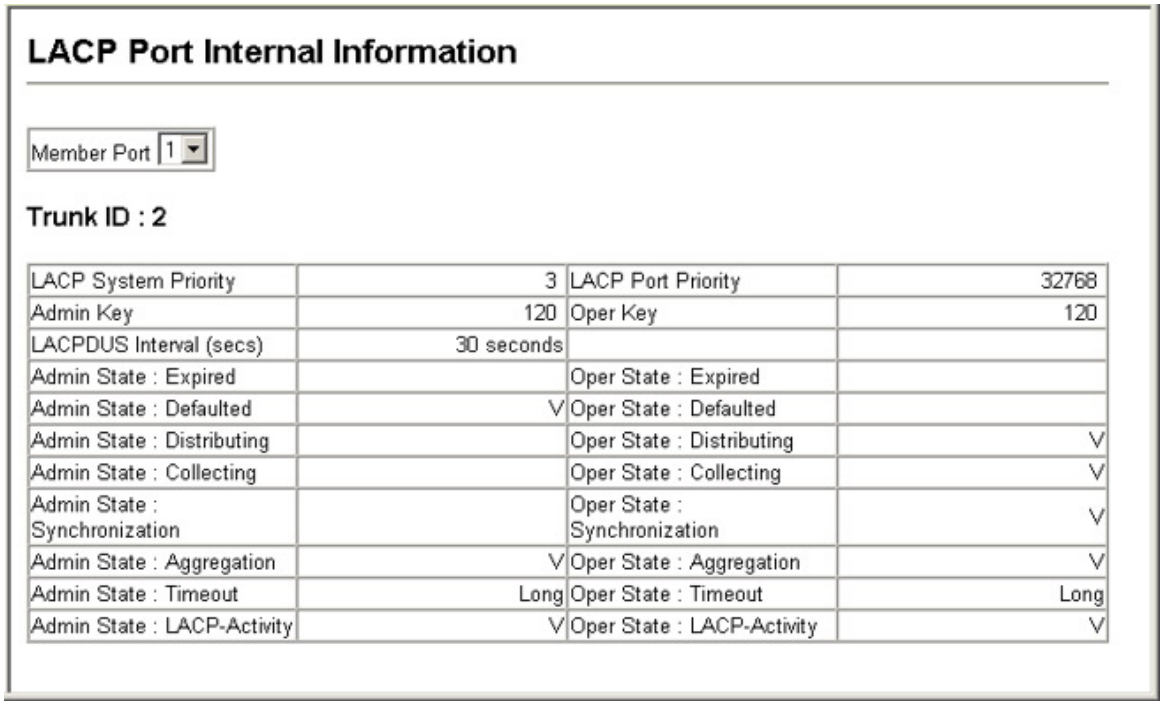
Field	Description
Oper Key	Current operational value of the key for the aggregation port.
Admin Key	Current administrative value of the key for the aggregation port.
LACPDUs Internal	Number of seconds before invalidating received LACPDU information.
LACP System Priority	LACP system priority assigned to this port channel.

Downloaded from www.Manualslib.com manuals search engine

Field	Description
LACP Port Priority	LACP port priority assigned to this interface within the channel group.
Admin State, Oper State	Administrative or operational values of the actor's state parameters: • Expired – The actor's receive machine is in the expired state; • Defaulted – The actor's receive machine is using defaulted operational partner information, administratively configured for the partner. • Distributing – If false, distribution of outgoing frames on this link is disabled; i.e., distribution is currently disabled and is not expected to be enabled in the absence of administrative changes or changes in received protocol information. • Collecting – Collection of incoming frames on this link is enabled; i.e., collection is currently enabled and is not expected to be disabled in the absence of administrative changes or changes in received protocol information. • Synchronization – The System considers this link to be IN_SYNC; i.e., it has been allocated to the correct Link Aggregation Group, the group has been associated with a compatible Aggregator, and the identity of the Link Aggregation Group is consistent with the System ID and operational Key information transmitted. • Aggregation – The system considers this link to be aggregatable; i.e., a potential candidate for aggregation. • Long timeout – Periodic transmission of LACPDUs uses a slow transmission rate. • LACP-Activity – Activity control value with regard to this link. (0: Passive; 1: Active)

Web – Click Port, LACP, Port Internal Information. Select a port channel to display the corresponding information.

Downloaded from www.Manualslib.com manuals search engine



LACP Port Internal Information

Member Port 1

Trunk ID : 2

LACP System Priority	3	LACP Port Priority	32768
Admin Key	120	Oper Key	120
LACPDUS Interval (secs)	30 seconds		
Admin State : Expired		Oper State : Expired	
Admin State : Defaulted	V	Oper State : Defaulted	
Admin State : Distributing		Oper State : Distributing	V
Admin State : Collecting		Oper State : Collecting	V
Admin State : Synchronization		Oper State : Synchronization	V
Admin State : Aggregation	V	Oper State : Aggregation	V
Admin State : Timeout	Long	Oper State : Timeout	Long
Admin State : LACP-Activity	V	Oper State : LACP-Activity	V

CLI – The following example displays the LACP configuration settings and operational state for the local side of port channel 1.

```
Console#show 1 lacp internal3-28
Channel group : 1
------------------------------------------------------------------------
Oper Key : 4
Admin Key : 0
Eth 1/1
------------------------------------------------------------------------
  LACPDUs Internal : 30 sec
  LACP System Priority : 32768
  LACP Port Priority : 32768
  Admin Key : 4
  Oper Key : 4
  Admin State : defaulted, aggregation, long timeout, LACP-activity
  Oper State : distributing, collecting, synchronization, aggregation,
               long timeout, LACP-activity
.
.
.
Console#
```

Displaying LACP Settings and Status for the Remote Side

You can display configuration settings and the operational state for the remote side of an link aggregation.

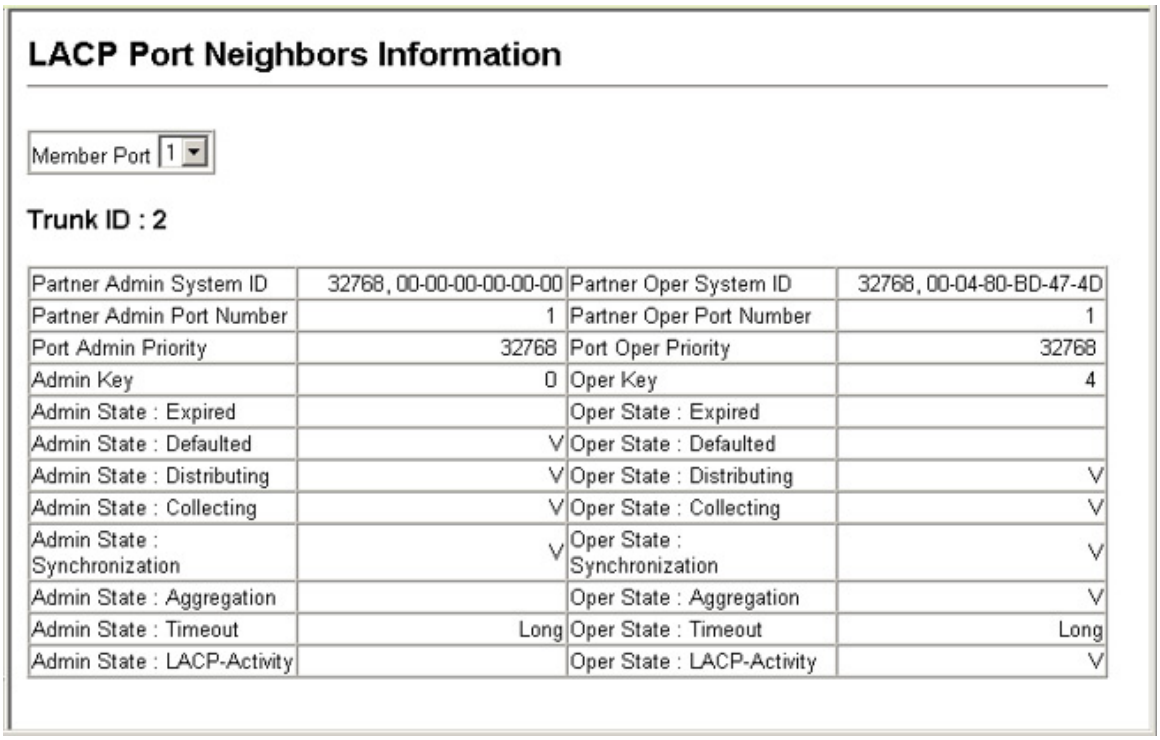
Downloaded from www.Manualslib.com manuals search engine

Neighbor Configuration Information

Field	Description
Partner Admin System ID	LAG partner's system ID assigned by the user.
Partner Oper System ID	LAG partner's system ID assigned by the LACP protocol.
Partner Admin Port Number	Current administrative value of the port number for the protocol Partner.
Partner Oper Port Number	Operational port number assigned to this aggregation port by the port's protocol partner.
Port Admin Priority	Current administrative value of the port priority for the protocol partner.
Port Oper Priority	Priority value assigned to this aggregation port by the partner.
Admin Key	Current administrative value of the Key for the protocol partner.
Oper Key	Current operational value of the Key for the protocol partner.
Admin State	Administrative values of the partner's state parameters. (See preceding table.)
Oper State	Operational values of the partner's state parameters. (See preceding table.)

Web – Click Port, LACP, Port Neighbors Information. Select a port channel to display the corresponding information.

Downloaded from www.Manualslib.com manuals search engine



LACP Port Neighbors Information

Member Port 1

Trunk ID : 2

Partner Admin System ID	32768, 00-00-00-00-00-00	Partner Oper System ID	32768, 00-04-80-BD-47-4D
Partner Admin Port Number	1	Partner Oper Port Number	1
Port Admin Priority	32768	Port Oper Priority	32768
Admin Key	0	Oper Key	4
Admin State : Expired		Oper State : Expired	
Admin State : Defaulted	V	Oper State : Defaulted	
Admin State : Distributing	V	Oper State : Distributing	V
Admin State : Collecting	V	Oper State : Collecting	V
Admin State : Synchronization	V	Oper State : Synchronization	V
Admin State : Aggregation		Oper State : Aggregation	V
Admin State : Timeout	Long	Oper State : Timeout	Long
Admin State : LACP-Activity		Oper State : LACP-Activity	V

CLI – The following example displays the LACP configuration settings and operational state for the remote side of port channel 1.

```
Console#show 1 lacp neighbors3-28
Channel group 1 neighbors
-------------------------------------------------------------------------
Eth 1/1
-------------------------------------------------------------------------
  Partner Admin System ID : 32768, 00-00-00-00-00-00
  Partner Oper System ID : 32768, 00-00-00-00-00-01
  Partner Admin Port Number : 1
  Partner Oper Port Number : 1
  Port Admin Priority : 32768
  Port Oper Priority : 32768
  Admin Key : 0
  Oper Key : 4
  Admin State : defaulted, distributing, collecting, synchronization,
                long timeout,
  Oper State : distributing, collecting, synchronization, aggregation,
               long timeout, LACP-activity
.
.
.
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Setting Broadcast Storm Thresholds

Broadcast storms may occur when a device on your network is malfunctioning, or if application programs are not well designed or properly configured. If there is too much broadcast traffic on your network, performance can be severely degraded or everything can come to complete halt.

You can protect your network from broadcast storms by setting a threshold for broadcast traffic for each port. Any broadcast packets exceeding the specified threshold will then be dropped.

Command Usage

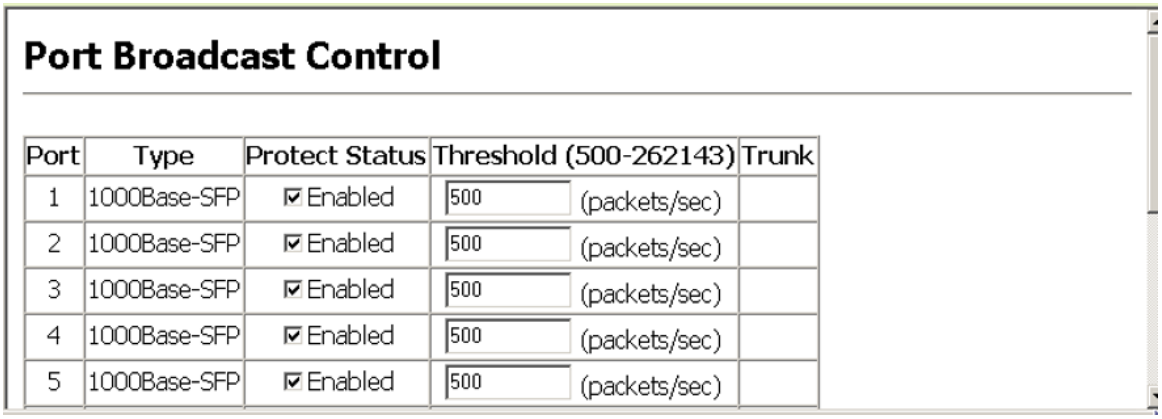
- Broadcast Storm Control is enabled by default.
- The default threshold is 500 packets per second.
- Broadcast control does not effect IP multicast traffic.
- The specified threshold applies to all ports on the switch.

Command Attributes

- **Protect Status** – Shows whether or not broadcast storm control has been enabled. (Default: Enabled)
- **Threshold** – Threshold as percentage of port bandwidth. (Options: 500-262143 packets per second; Default: 500 packets per second)

Web – Click Port, Port Broadcast Control. Set the threshold any port, click Apply.

Downloaded from www.Manualslib.com manuals search engine



Port Broadcast Control

Port	Type	Protect Status	Threshold (500-262143)	Trunk
1	1000Base-SFP	☑ Enabled	500 (packets/sec)	
2	1000Base-SFP	☑ Enabled	500 (packets/sec)	
3	1000Base-SFP	☑ Enabled	500 (packets/sec)	
4	1000Base-SFP	☑ Enabled	500 (packets/sec)	
5	1000Base-SFP	☑ Enabled	500 (packets/sec)	

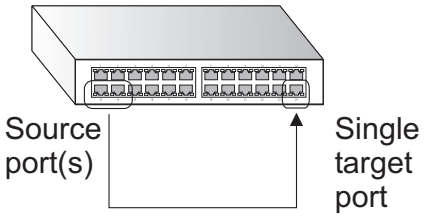
CLI – Specify any interface, and then enter the threshold. The following disables broadcast storm control for port 1, and then sets broadcast suppression at 600 packets per second for port 2.

```
Console(config)#interface ethernet 1/13-1
Console(config-if)#no switchport broadcast3-9
Console(config-if)#exit
Console(config)#interface ethernet 1/2
Console(config-if)#switchport broadcast packet-rate 6003-9
Console(config-if)#end
Console#show interfaces switchport ethernet 1/23-14
Information of Eth 1/2
 Broadcast threshold: Enabled, 600 packets/second
 Lacp status: Disabled
 Ingress rate limit: disable,1000M bits per second
 Egress rate limit: disable,1000M bits per second
 VLAN membership mode: Hybrid
 Ingress rule: Disabled
 Acceptable frame type: All frames
 Native VLAN: 1
 Priority for untagged traffic: 0
 Gvrp status: Disabled
 Allowed Vlan:    1(u),
 Forbidden Vlan:
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Configuring Port Mirroring

You can mirror traffic from any source port to a target port for real-time analysis. You can then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner.



Command Usage

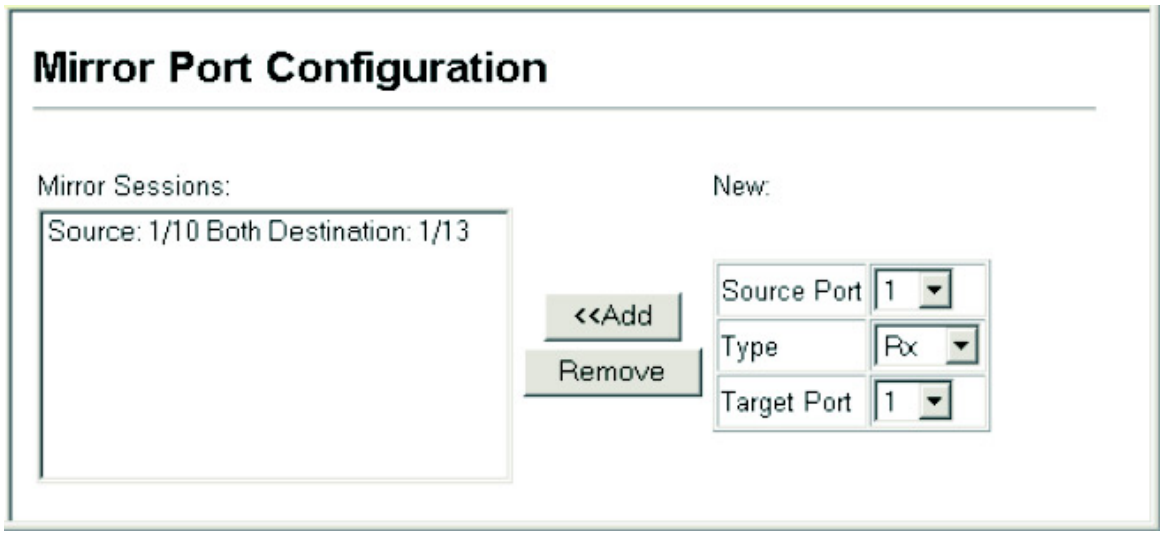
- Monitor port speed should match or exceed source port speed, otherwise traffic may be dropped from the monitor port.
- All mirror sessions have to share the same destination port.
- When mirroring port traffic, the target port must be included in the same VLAN as the source port.

Command Attributes

- **Mirror Sessions** – Displays a list of current mirror sessions.
- **Source Port** – The port whose traffic will be monitored.
- **Type** – Allows you to select which traffic to mirror to the target port, Rx (receive), Tx (transmit), or Both.
- **Target Port** – The port that will "duplicate" or "mirror" the traffic on the source port.

Web – Click Port, Mirror. Specify the source port, the traffic type to be mirrored, and the monitor port, then click Add.

Downloaded from www.Manualslib.com manuals search engine



CLI – Use the interface command to select the monitor port, then use the port monitor command to specify the source port. Note that default mirroring under the CLI is for both received and transmitted packets.

```
Console(config)#interface ethernet 1/103-1
Console(config-if)#port monitor ethernet 1/133-16
Console(config-if)#
```


Downloaded from www.Manualslib.com manuals search engine

Configuring Rate Limits

This function allows the network manager to control the maximum rate for traffic transmitted or received on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic into or out of the switch. Traffic that falls within the rate limit is transmitted, while packets that exceed the acceptable amount of traffic are dropped.

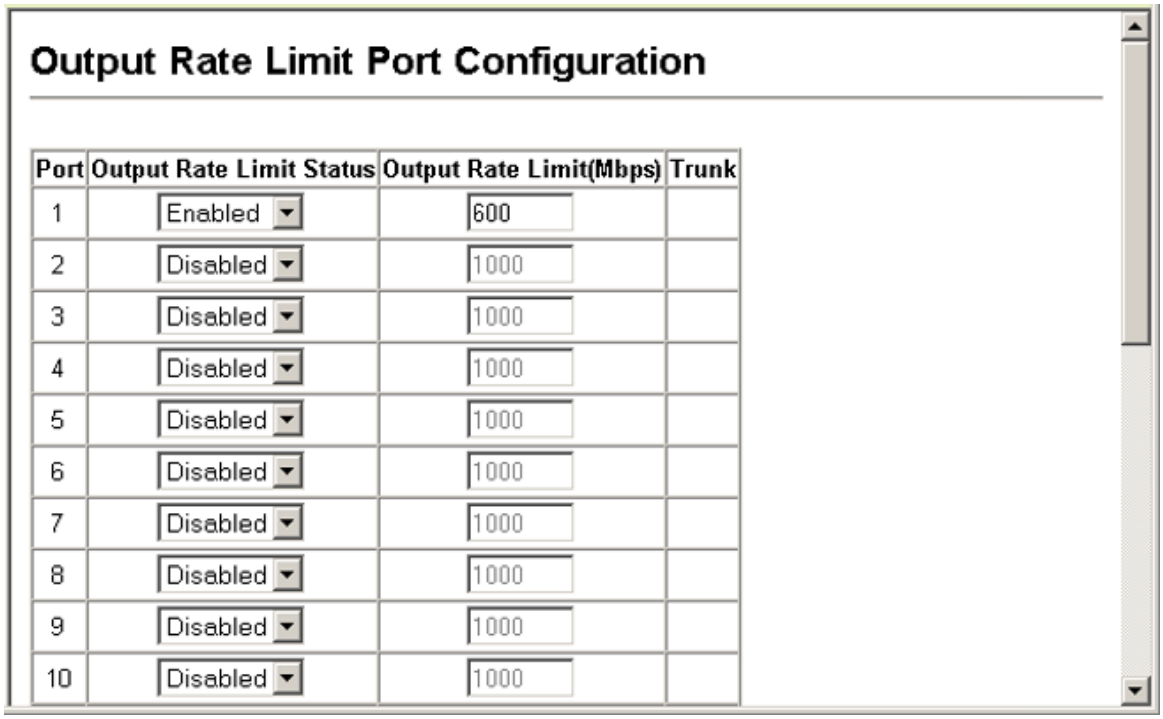
Rate limiting can be applied to individual ports or trunks. When an interface is configured with this feature, the traffic rate will be monitored by the hardware to verify conformity. Non-conforming traffic is dropped, conforming traffic is forwarded without any changes.

Command Attribute

- **Rate Limit** – Sets the output rate limit for an interface.
  Default Status – Disabled
  Default Rate – 1000 Mbps
  Range – 1 - 1000 Mbps

Downloaded from www.Manualslib.com manuals search engine

Web - Click Rate Limit, Input/Output Port/Trunk Configuration. Set the Input Rate Limit Status or Output Rate Limit Status, then set the rate limit for the individual interfaces, and click Apply.



Output Rate Limit Port Configuration

Port	Output Rate Limit Status	Output Rate Limit(Mbps)	Trunk
1	Enabled	600	
2	Disabled	1000	
3	Disabled	1000	
4	Disabled	1000	
5	Disabled	1000	
6	Disabled	1000	
7	Disabled	1000	
8	Disabled	1000	
9	Disabled	1000	
10	Disabled	1000	

CLI - This example sets the rate limit for input and output traffic passing through port 1 to 600 Mbps.

```
Console(config)#interface ethernet 1/13-1
Console(config-if)#rate-limit input 6003-19
Console(config-if)#rate-limit output 600
Console(config-if)#
```

Showing Port Statistics

You can display standard statistics on network traffic from the Interfaces Group and Ethernet-like MIBs, as well as a detailed breakdown of traffic based on the RMON MIB. Interfaces and Ethernet-like statistics display errors on the traffic passing through each port. This information can be used to identify potential problems with the switch (such as a faulty port or unusually heavy loading). RMON statistics provide access to a broad range of statistics, including a total count of different frame types and sizes passing through each port. All values displayed have been accumulated

Downloaded from www.Manualslib.com manuals search engine

since the last system reboot, and are shown as counts per second. Statistics are refreshed every 60 seconds by default.

Note: RMON groups 2, 3 and 9 can only be accessed using SNMP management software such as HP OpenView.

Statistical Values

Parameter	Description
Interface Statistics	
Received Octets	The total number of octets received on the interface, including framing characters.
Received Unicast Packets	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Received Multicast Packets	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a multicast address at this sub-layer.
Received Broadcast Packets	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a broadcast address at this sub-layer.
Received Discarded Packets	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
Received Unknown Packets	The number of packets received via the interface which were discarded because of an unknown or unsupported protocol.
Received Errors	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Transmit Octets	The total number of octets transmitted out of the interface, including framing characters.
Transmit Unicast Packets	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.

Downloaded from www.Manualslib.com manuals search engine

Parameter	Description
Transmit Multicast Packets	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent.
Transmit Broadcast Packets	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent.
Transmit Discarded Packets	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
Transmit Errors	The number of outbound packets that could not be transmitted because of errors.
Etherlike Statistics	
Alignment Errors	The number of alignment errors (missynchronized data packets).
Late Collisions	The number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
FCS Errors	A count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check. This count does not include frames received with frame-too-long or frame-too-short error.
Excessive Collisions	A count of frames for which transmission on a particular interface fails due to excessive collisions. This counter does not increment when the interface is operating in full-duplex mode.
Single Collision Frames	The number of successfully transmitted frames for which transmission is inhibited by exactly one collision.
Internal MAC Transmit Errors	A count of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error.
Multiple Collision Frames	A count of successfully transmitted frames for which transmission is inhibited by more than one collision.

Downloaded from www.Manualslib.com manuals search engine

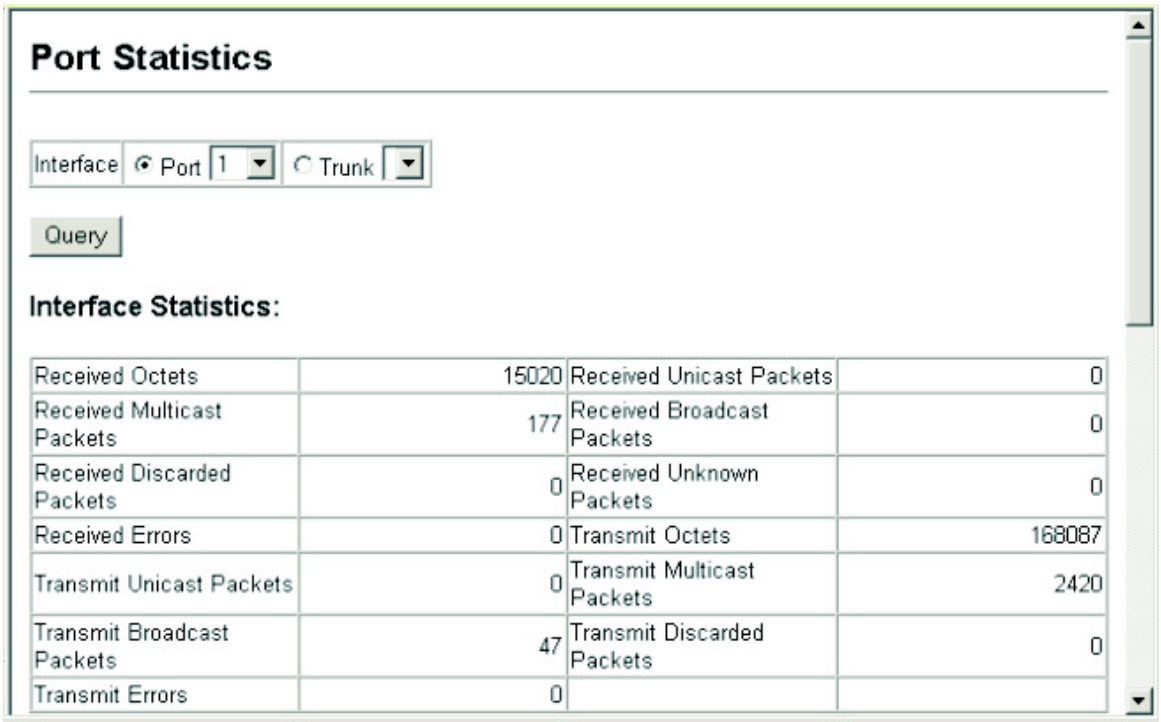
Parameter	Description
Carrier Sense Errors	The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame.
SQE Test Errors	A count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface.
Frames Too Long	A count of frames received on a particular interface that exceed the maximum permitted frame size.
Deferred Transmissions	A count of frames for which the first transmission attempt on a particular interface is delayed because the medium was busy.
Internal MAC Receive Errors	A count of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error.
RMON Statistics	
Drop Events	The total number of events in which packets were dropped due to lack of resources.
Jabbers	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS or alignment error.
Received Bytes	Total number of bytes of data received on the network. This statistic can be used as a reasonable indication of Ethernet utilization.
Collisions	The best estimate of the total number of collisions on this Ethernet segment.
Received Frames	The total number of frames (bad, broadcast and multicast) received.
Broadcast Frames	The total number of good frames received that were directed to the broadcast address. Note that this does not include multicast packets.
Multicast Frames	The total number of good frames received that were directed to this multicast address.
CRC/Alignment Errors	The number of CRC/alignment errors (FCS or alignment errors).
Undersize Frames	The total number of frames received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.

Downloaded from www.Manualslib.com manuals search engine

Parameter	Description
Oversize Frames	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
Fragments	The total number of frames received that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS or alignment error.
64 Bytes Frames	The total number of frames (including bad packets) received and transmitted that were 64 octets in length (excluding framing bits but including FCS octets).
65-127 Byte Frames 128-255 Byte Frames 256-511 Byte Frames 512-1023 Byte Frames 1024-1518 Byte Frames 1519-1536 Byte Frames	The total number of frames (including bad packets) received and transmitted where the number of octets fall within the specified range (excluding framing bits but including FCS octets).

Web – Click Port, Port Statistics. Select the required interface, and click Query. You can also use the Refresh button at the bottom of the page to update the screen.

Downloaded from www.Manualslib.com manuals search engine



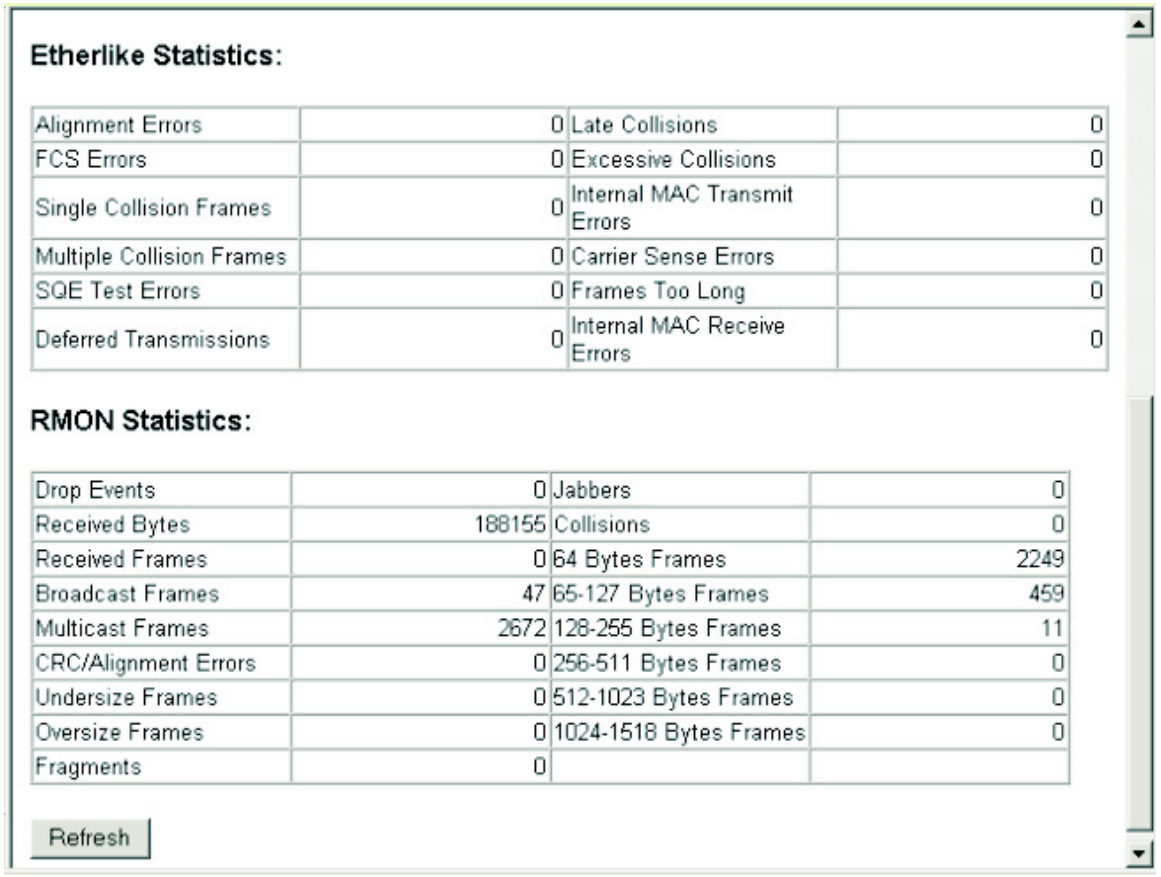
Port Statistics

Interface ◉ Port 1 ○ Trunk

Query

Interface Statistics:

Received Octets	15020	Received Unicast Packets	0
Received Multicast Packets	177	Received Broadcast Packets	0
Received Discarded Packets	0	Received Unknown Packets	0
Received Errors	0	Transmit Octets	168087
Transmit Unicast Packets	0	Transmit Multicast Packets	2420
Transmit Broadcast Packets	47	Transmit Discarded Packets	0
Transmit Errors	0		



Etherlike Statistics:

Alignment Errors	0	Late Collisions	0
FCS Errors	0	Excessive Collisions	0
Single Collision Frames	0	Internal MAC Transmit Errors	0
Multiple Collision Frames	0	Carrier Sense Errors	0
SQE Test Errors	0	Frames Too Long	0
Deferred Transmissions	0	Internal MAC Receive Errors	0

RMON Statistics:

Drop Events	0	Jabbers	0
Received Bytes	188155	Collisions	0
Received Frames	0	64 Bytes Frames	2249
Broadcast Frames	47	65-127 Bytes Frames	459
Multicast Frames	2672	128-255 Bytes Frames	11
CRC/Alignment Errors	0	256-511 Bytes Frames	0
Undersize Frames	0	512-1023 Bytes Frames	0
Oversize Frames	0	1024-1518 Bytes Frames	0
Fragments	0		

Refresh

Downloaded from www.Manualslib.com manuals search engine

CLI – This example shows statistics for port 12.

```
Console#show interfaces counters ethernet 1/123-13
Ethernet 1/12
 Iftable stats:
  Octets input: 868453, Octets output: 3492122
  Unicast input: 7315, Unitcast output: 6658
  Discard input: 0, Discard output: 0
  Error input: 0, Error output: 0
  Unknown protos input: 0, QLen output: 0
 Extended iftable stats:
  Multi-cast input: 0, Multi-cast output: 17027
  Broadcast input: 231, Broadcast output: 7
 Ether-like stats:
  Alignment errors: 0, FCS errors: 0
  Single Collision frames: 0, Multiple collision frames: 0
  SQE Test errors: 0, Deferred transmissions: 0
  Late collisions: 0, Excessive collisions: 0
  Internal mac transmit errors: 0, Internal mac receive errors: 0
  Frame too longs: 0, Carrier sense errors: 0
  Symbol errors: 0
 RMON stats:
  Drop events: 0, Octets: 4422579, Packets: 31552
  Broadcast pkts: 238, Multi-cast pkts: 17033
  Undersize pkts: 0, Oversize pkts: 0
  Fragments: 0, Jabbers: 0
  CRC align errors: 0, Collisions: 0
  Packet size <= 64 octets: 25568, Packet size 65 to 127 octets: 1616
  Packet size 128 to 255 octets: 1249, Packet size 256 to 511 octets: 1449
  Packet size 512 to 1023 octets: 802, Packet size 1024 to 1518 octets: 871
```

Address Table Settings

Switches store the addresses for all known devices. This information is used to pass traffic directly between the inbound and outbound ports. All the addresses learned by monitoring traffic are stored in the dynamic address table. You can also manually configure static addresses that are bound to a specific port.

Setting Static Addresses

A static address can be assigned to a specific interface on this switch. Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table.

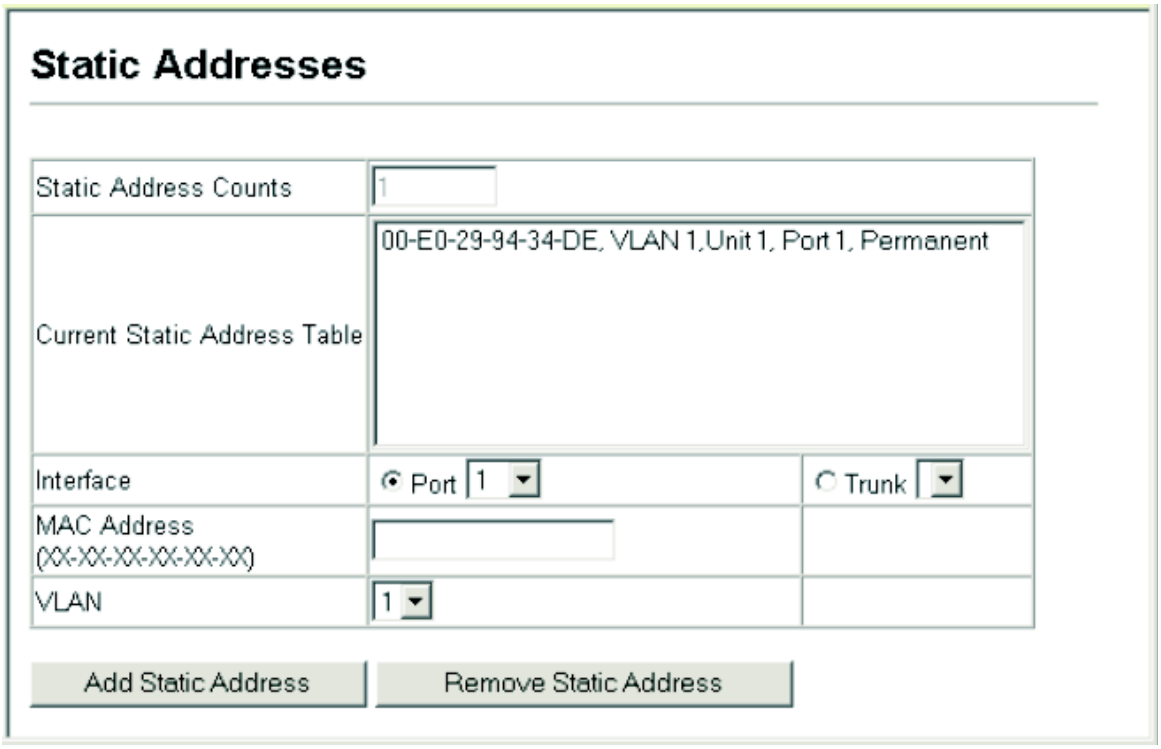
Downloaded from www.Manualslib.com manuals search engine

Command Attributes

- **Static Address Counts*** – The number of manually configured addresses.
- **Current Static Address Table** – Lists all the static addresses.
- **Interface** – Port or trunk associated with the device assigned a static address.
- **MAC Address** – Physical address of a device mapped to this interface.
- **VLAN** – ID of configured VLAN (1-4094).

* Web Only

Web – Click Address Table, Static Addresses. Specify the interface, the MAC address and VLAN, then click Add Static Address.



Downloaded from www.Manualslib.com manuals search engine

CLI – This example adds an address to the static address table, but sets it to be deleted when the switch is reset.

```
Console(config)#mac-address-table static 00-e0-29-94-34-de interface
ethernet 1/1 vlan 1 delete-on-reset3-34
Console(config)#
```

Displaying the Address Table

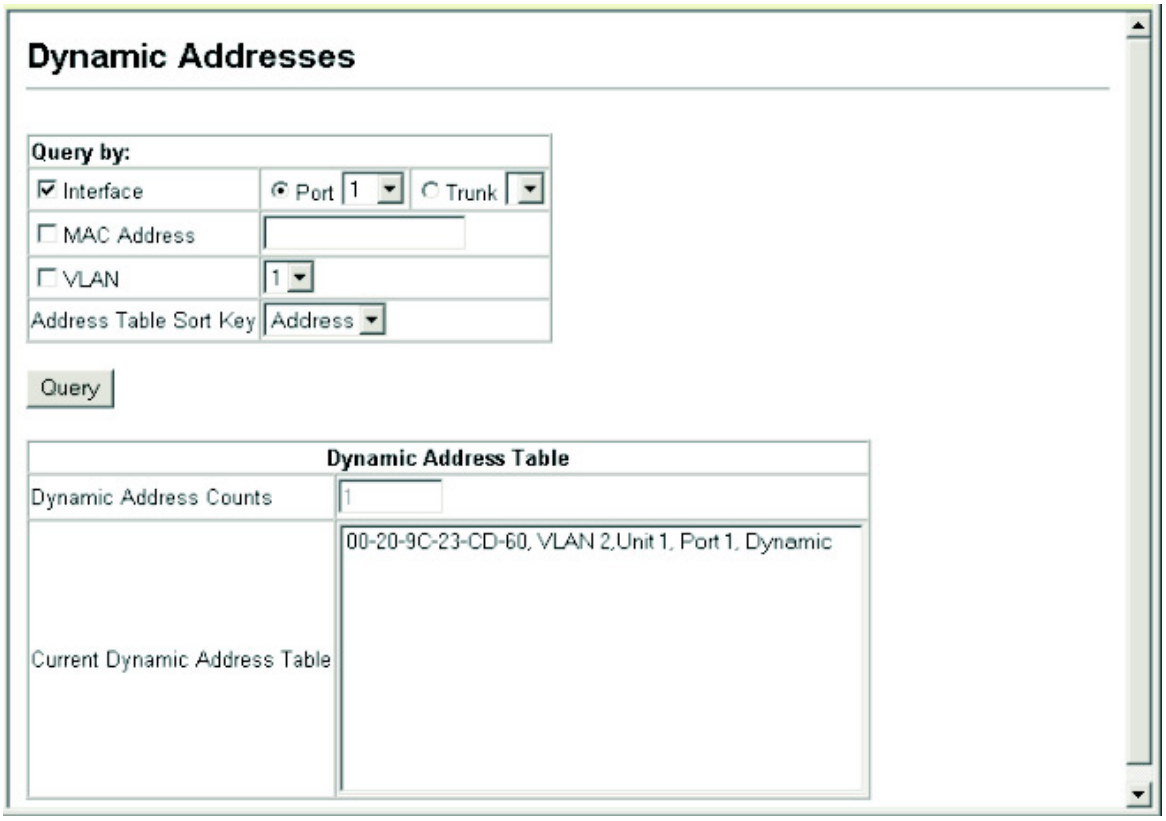
The Dynamic Address Table contains the MAC addresses learned by monitoring the source address for traffic entering the switch. When the destination address for inbound traffic is found in the database, the packets intended for that address are forwarded directly to the associated port. Otherwise, the traffic is flooded to all ports.

Command Attributes

- **Interface** – Indicates a port or trunk.
- **MAC Address** – Physical address associated with this interface.
- **VLAN** – ID of configured VLAN (1-4094).
- **Address Table Sort Key** – You can sort the information displayed based on MAC address, VLAN or interface (port or trunk).

Web – Click Address Table, Dynamic Addresses. Specify the search type (i.e., mark the Interface, MAC Address, or VLAN checkbox), select the method of sorting the displayed addresses, and then click Query.

Downloaded from www.Manualslib.com manuals search engine



CLI – This example also displays the address table entries for port 1.

```
Console#show mac-address-table interface ethernet 1/13-35
 Interface Mac Address       Vlan Type
 --------- ----------------- ---- -----------------
  Eth 1/ 1 00-E0-29-94-34-DE    1 Permanent
  Eth 1/ 1 00-20-9C-23-CD-60    2 Learned
Console#
```

Changing the Aging Time

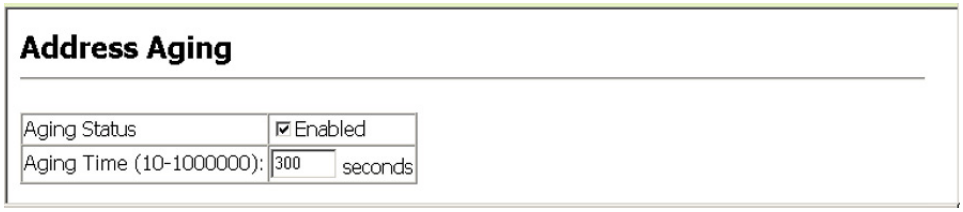
You can set the aging time for entries in the dynamic address table.

Command Attributes

- **Aging Time** – The time after which a learned entry is discarded. (Range: 10-1000000 seconds; Default: 300 seconds)

Web – Click Address Table, Address Aging. Specify the new aging time, click Apply.

Downloaded from www.Manualslib.com manuals search engine



CLI – This example sets the aging time to 400 seconds.

```
Console(config)#mac-address-table aging-time 4003-36
Console(config)#
```

Spanning Tree Algorithm Configuration

The Spanning Tree Algorithm (STA) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STA-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

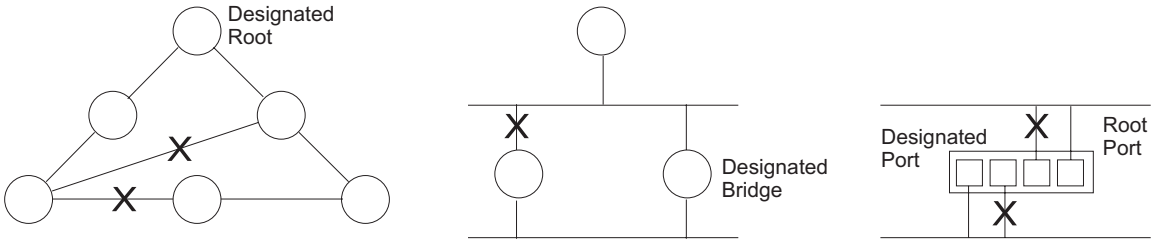
The spanning tree algorithms supported by this switch include these versions:

- STP – Spanning Tree Protocol (IEEE 802.1D)
- RSTP – Rapid Spanning Tree Protocol (IEEE 802.1w)

STA uses a distributed algorithm to select a bridging device (STA-compliant switch, bridge or router) that serves as the root of the spanning tree network. It selects a root port on each bridging device (except for the root device) which incurs the lowest path cost when forwarding a packet from that device to the root device. Then it selects a designated bridging device from each LAN which incurs the lowest path cost when forwarding a packet from that LAN to the root device. All ports connected to designated bridging devices are assigned as designated ports. After determining the lowest cost spanning tree, it enables all root ports and designated ports, and disables all other ports. Network packets are

Downloaded from www.Manualslib.com manuals search engine

therefore only forwarded between root ports and designated ports, eliminating any possible network loops.



Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the Root Bridge. If a bridge does not get a Hello BPDU after a predefined interval (Maximum Age), the bridge assumes that the link to the Root Bridge is down. This bridge will then initiate negotiations with other bridges to reconfigure the network to reestablish a valid network topology.

RSTP is designed as a general replacement for the slower, legacy STP. RSTP achieves must faster reconfiguration (i.e., around one tenth of the time required by STP) by reducing the number of state changes before active ports start learning, predefining an alternate route that can be used when a node or port fails, and retaining the forwarding database for ports insensitive to changes in the tree structure when reconfiguration occurs.

Displaying Global Settings

You can display a summary of the current bridge STA information that applies to the entire switch using the STA Information screen.

Field Attributes

- **Spanning Tree State** – Shows if the switch is enabled to participate in an STA-compliant network.
- **Bridge ID** – A unique identifier for this bridge, consisting of the bridge priority and MAC address (where the address is taken from the switch system).

Downloaded from www.Manualslib.com manuals search engine

- **Max Age** – The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network. (References to "ports" in this section mean "interfaces," which includes both ports and trunks.)

- **Hello Time** – Interval (in seconds) at which the root device transmits a configuration message.

- **Forward Delay** – The maximum time (in seconds) the root device will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.

- **Designated Root** – The priority and MAC address of the device in the Spanning Tree that this switch has accepted as the root device.

    - **Root Port** – The number of the port on this switch that is closest to the root. This switch communicates with the root device through this port. If there is no root port, then this switch has been accepted as the root device of the Spanning Tree network.
    - **Root Path Cost** – The path cost from the root port on this switch to the root device.
- **Configuration Changes** – The number of times the Spanning Tree has been reconfigured.

- **Last Topology Change** – Time since the Spanning Tree was last reconfigured.

Downloaded from www.Manualslib.com manuals search engine

These additional parameters are only displayed for the CLI:

- **Spanning tree mode** – Specifies the type of spanning tree used on this switch:

  - **STP**: Spanning Tree Protocol (IEEE 802.1D)
  - **RSTP**: Rapid Spanning Tree (IEEE 802.1w)
  -

- **Instance*** –

- **Vlans configuration** – VLANs assigned to the CIST.

- **Priority** – Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.

- **Root Hello Time** – Interval (in seconds) at which this device transmits a configuration message.

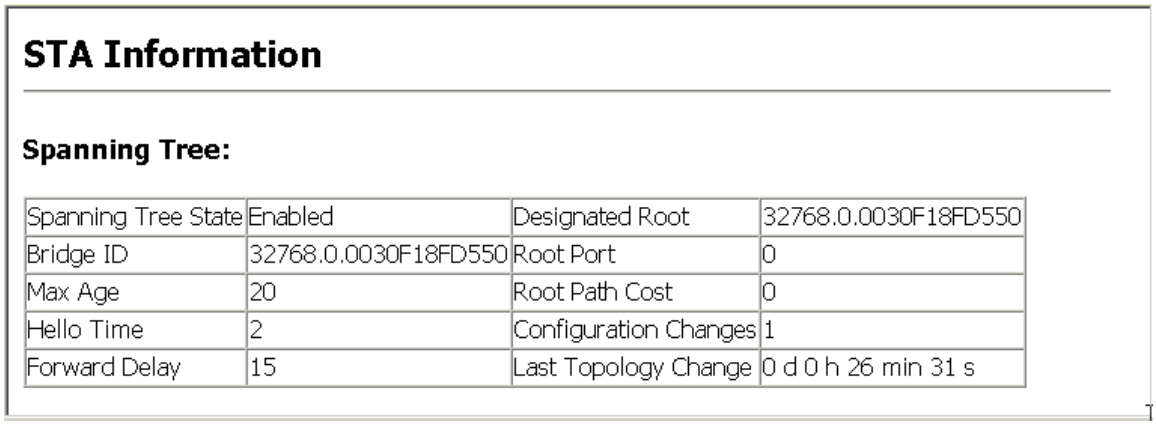
- **Root Maximum Age** – The maximum time (in seconds) this device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. If the root port ages out STA information (provided in the last configuration message), a new root port is selected from among the device ports attached to the network. (References to "ports" in this section means "interfaces," which includes both ports and trunks.)

- **Root Forward Delay** – The maximum time (in seconds) this device will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.

Downloaded from www.Manualslib.com manuals search engine

- **Root Hold Time** – The interval (in seconds) during which no more than two bridge configuration protocol data units shall be transmitted by this node.
- **Max hops** – The max number of hop counts for the MST region.
- **Remaining hops** – The remaining number of hop counts for the MST instance.
- **Transmission limit** – The minimum interval between the transmission of consecutive RSTP/MSTP BPDUs.
- **Path Cost Method** – The path cost is used to determine the best path between devices. The path cost method is used to determine the range of values that can be assigned to each interface.

Web – Click Spanning Tree, STA, Information.



STA Information

Spanning Tree:

Spanning Tree State	Enabled	Designated Root	32768.0.0030F18FD550
Bridge ID	32768.0.0030F18FD550	Root Port	0
Max Age	20	Root Path Cost	0
Hello Time	2	Configuration Changes	1
Forward Delay	15	Last Topology Change	0 d 0 h 26 min 31 s

Downloaded from www.Manualslib.com manuals search engine

CLI – This command displays global STA settings, followed by settings for each port.

```
Console#show spanning-tree3-51
Spanning-tree information
---------------------------------------------------------------
 Spanning tree mode               :MSTP
 Spanning tree enable/disable     :enable
 Instance                         :0
 VLANs configuration              :1-4094
 Priority                         :32768
 Bridge Hello Time (sec.)         :2
 Bridge Max Age (sec.)            :20
 Bridge Forward Delay (sec.)      :15
 Root Hello Time (sec.)           :2
 Root Max Age (sec.)              :20
 Root Forward Delay (sec.)        :15
 Max hops                         :20
 Remaining hops                   :20
 Designated Root                  :32768.0.0030F18FD550
 Current root port                :0
 Current root cost                :0
 Number of topology changes       :1
 Last topology changes time (sec.):1762
 Transmission limit               :3
 Path Cost Method                 :long.
.
.
```

Note: The current root port and current root cost display as zero when this device is not connected to the network.

Configuring Global Settings

Global settings apply to the entire switch.

Command Usage

- Spanning Tree Protocol

- Uses RSTP for the internal state machine, but sends only 802.1D BPDUs. Rapid Spanning Tree Protocol

  RSTP supports connections to either STP or RSTP nodes by monitoring the incoming protocol messages and dynamically adjusting the type of protocol messages the RSTP node transmits, as described below:

Downloaded from www.Manualslib.com manuals search engine

- STP Mode – If the switch receives an 802.1D BPDU (i.e., STP BPDU) after a port's migration delay timer expires, the switch assumes it is connected to an 802.1D bridge and starts using only 802.1D BPDUs.
- RSTP Mode – If RSTP is using 802.1D BPDUs on a port and receives an RSTP BPDU after the migration delay expires, RSTP restarts the migration delay timer and begins using RSTP BPDUs on that port.

-

Command Attributes

Basic Configuration of Global Settings

- **Spanning Tree State** – Enables/disables STA on this switch. (Default: Enabled)

- **Spanning Tree Type** – Specifies the type of spanning tree used on this switch:

  - **STP**: Spanning Tree Protocol (IEEE 802.1D); i.e., when this option is selected, the switch will use RSTP set to STP forced compatibility mode).
  - **RSTP**: Rapid Spanning Tree (IEEE 802.1w); RSTP is the default.
  -

- **Priority** – Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device. (Note that lower numeric values indicate higher priority.)

  - Default: 32768
  - Range: 0-61440, in steps of 4096
  - Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440

Downloaded from www.Manualslib.com manuals search engine

Root Device Configuration

- **Hello Time** – Interval (in seconds) at which the root device transmits a configuration message.

  - Default: 2
  - Minimum: 1
  - Maximum: The lower of 10 or [(Max. Message Age / 2) -1]

- **Maximum Age** – The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network. (References to "ports" in this section mean "interfaces," which includes both ports and trunks.)

  - Default: 20
  - Minimum: The higher of 6 or [2 x (Hello Time + 1)].
  - Maximum: The lower of 40 or [2 x (Forward Delay - 1)]

- **Forward Delay** – The maximum time (in seconds) this device will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.

  - Default: 15
  - Minimum: The higher of 4 or [(Max. Message Age / 2) + 1]
  - Maximum: 30

Configuration Settings for RSTP

- **Path Cost Method** – The path cost is used to determine the best path

Downloaded from www.Manualslib.com manuals search engine

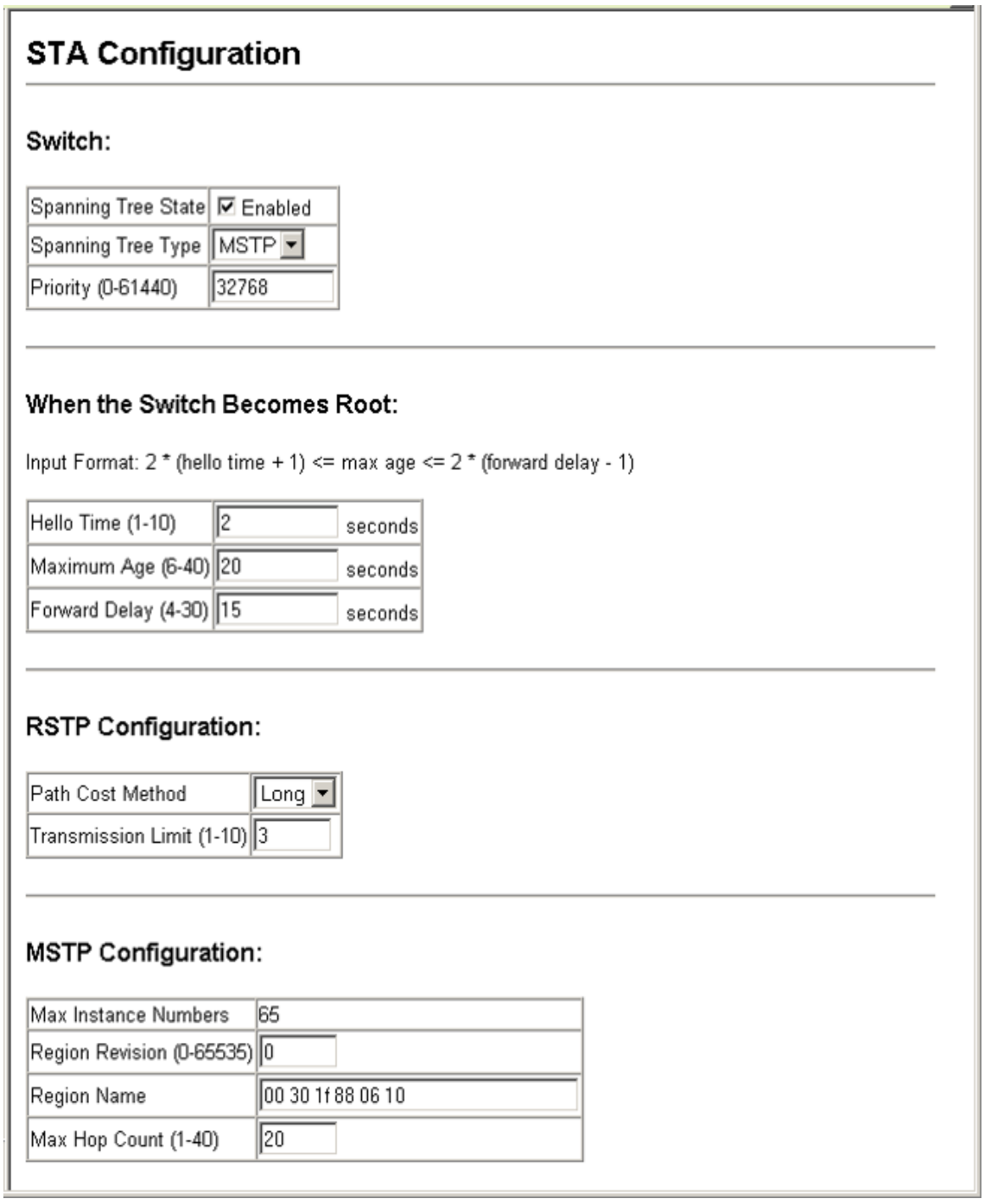
between devices. The path cost method is used to determine the range of values that can be assigned to each interface.

  - Long: Specifies 32-bit based values that range from 1-200,000,000. (This is the default.)
  - Short: Specifies 16-bit based values that range from 1-65535.
- **Transmission Limit** – The maximum transmission rate for BPDUs is specified by setting the minimum interval between the transmission of consecutive protocol messages. (Range: 1-10; Default: 3)

Configuration Settings for MSTP

Downloaded from www.Manualslib.com manuals search engine

Web – Click Spanning Tree, STA, Configuration. Modify the required attributes, and click Apply.



Downloaded from www.Manualslib.com manuals search engine

CLI – This example enables Spanning Tree Protocol, sets the mode to MST, and then configures the STA and MSTP parameters.

```
Console(config)#spanning-tree3-39
Console(config)#spanning-tree mode mst3-39
Console(config)#spanning-tree priority 400003-43
Console(config)#spanning-tree hello-time 53-42
Console(config)#spanning-tree max-age 383-42
Console(config)#spanning-tree forward-time 203-41
Console(config)#spanning-tree pathcost method long3-44
Console(config)#spanning-tree transmission-limit 43-45
Console(config)#4-168
4-1714-1704-172
```

Displaying Interface Settings

The STA Port Information and STA Trunk Information pages display the current status of ports and trunks in the Spanning Tree.

Field Attributes

- **Spanning Tree** – Shows if STA has been enabled on this interface.
- **STA Status** – Displays current state of this port within the Spanning Tree:
  - **Discarding** - Port receives STA configuration messages, but does not forward packets.
  - **Learning** - Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses.
  - **Forwarding** - Port forwards packets, and continues learning addresses.

The rules defining port status are:

- A port on a network segment with no other STA compliant bridging device is always forwarding.
- If two ports of a switch are connected to the same segment and there is no other STA device attached to this segment, the port with the smaller ID forwards packets and the other is discarding.

Downloaded from www.Manualslib.com manuals search engine

- All ports are discarding when the switch is booted, then some of them change state to learning, and then to forwarding.

- **Forward Transitions** – The number of times this port has transitioned from the Learning state to the Forwarding state.

- **Designated Cost** – The cost for a packet to travel from this port to the root in the current Spanning Tree configuration. The slower the media, the higher the cost.

- **Designated Bridge** – The bridge priority and MAC address of the device through which this port must communicate to reach the root of the Spanning Tree.

- **Designated Port** – The port priority and number of the port on the designated bridging device through which this switch must communicate with the root of the Spanning Tree.

- **Oper Link Type** – The operational point-to-point status of the LAN segment attached to this interface. This parameter is determined by manual configuration or by auto-detection, as described for Admin Link Type in STA Port Configuration on page 3-140.

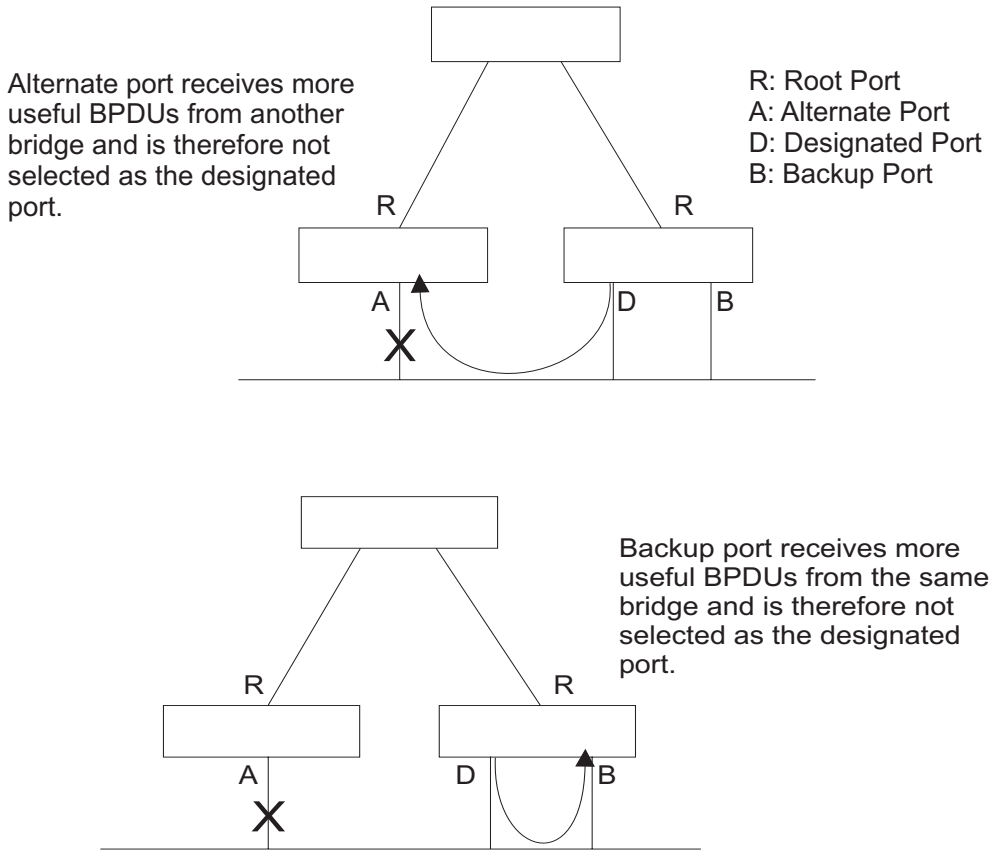
- **Oper Edge Port** – This parameter is initialized to the setting for Admin Edge Port in STA Port Configuration on page 3-140 (i.e., true or false), but will be set to false if a BPDU is received, indicating that another bridge is attached to this port.

- **Port Role** – Roles are assigned according to whether the port is part of the active topology connecting the bridge to the root bridge (i.e., **root** port), connecting a LAN through the bridge to the root bridge (i.e., **designated** port); or is an **alternate** or **backup** port that may provide connectivity if other bridges, bridge ports, or LANs fail or are removed. The role is set to disabled (i.e., **disabled** port) if a port has no role within the spanning tree.

- **Trunk Member** – Indicates if a port is a member of a trunk.

Downloaded from www.Manualslib.com manuals search engine

(STA Port Information only)



These additional parameters are only displayed for the CLI:

- **Admin status** – Shows if this interface is enabled.
- **External path cost** – The path cost for the IST. This parameter is used by the STA to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. (Path cost takes precedence over port priority.)
- **Internal path cost** – The path cost for the MST. See the preceeding item.
- **Priority** – Defines the priority used for this port in the Spanning Tree Algorithm. If the path cost for all ports on a switch is the same, the port with the highest priority (i.e., lowest value) will be configured as

Downloaded from www.Manualslib.com manuals search engine

an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Algorithm is detecting network loops. Where more than one port is assigned the highest priority, the port with the lowest numeric identifier will be enabled.

- **Designated root** – The priority and MAC address of the device in the Spanning Tree that this switch has accepted as the root device.

- **Fast forwarding** – This field provides the same information as Admin Edge port, and is only included for backward compatibility with earlier products.

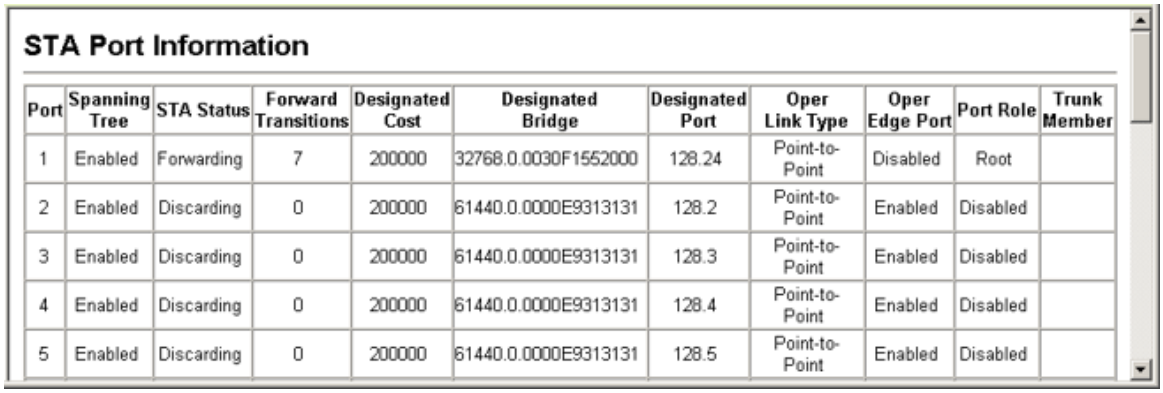
- **Admin Edge Port** – You can enable this option if an interface is attached to a LAN segment that is at the end of a bridged LAN or to an end node. Since end nodes **cannot** cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying Edge Ports provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to reconfigure when the interface changes state, and also overcomes other STA-related timeout problems. However, remember that Edge Port should only be enabled for ports connected to an end-node device.

- **Admin Link Type** – The link type attached to this interface.

    - Point-to-Point – A connection to exactly one other bridge.
    - Shared – A connection to two or more bridges.
    - Auto – The switch automatically determines if the interface is attached to a point-to-point link or to shared media.

Downloaded from www.Manualslib.com manuals search engine

Web – Click Spanning Tree, STA, Port Information or STA Trunk Information.



STA Port Information

Port	Spanning Tree	STA Status	Forward Transitions	Designated Cost	Designated Bridge	Designated Port	Oper Link Type	Oper Edge Port	Port Role	Trunk Member
1	Enabled	Forwarding	7	200000	32768.0.0030F1552000	128.24	Point-to-Point	Disabled	Root	
2	Enabled	Discarding	0	200000	61440.0.0000E9313131	128.2	Point-to-Point	Enabled	Disabled	
3	Enabled	Discarding	0	200000	61440.0.0000E9313131	128.3	Point-to-Point	Enabled	Disabled	
4	Enabled	Discarding	0	200000	61440.0.0000E9313131	128.4	Point-to-Point	Enabled	Disabled	
5	Enabled	Discarding	0	200000	61440.0.0000E9313131	128.5	Point-to-Point	Enabled	Disabled	

CLI – This example shows the STA attributes for port 5.

```
Console#show spanning-tree ethernet 1/53-51
Eth  1/ 5 information
---------------------------------------------------------------
 Admin status          : enable
 Role                  : disable
 State                 : discarding
 External path cost    : 10000
 Internal path cost    : 10000
 Priority              : 128
 Designated cost       : 200000
 Designated port       : 128.5
 Designated root       : 61440.0.0000E9313131
 Designated bridge     : 61440.0.0000E9313131
 Fast forwarding       : enable
 Forward transitions   : 0
 Admin edge port       : enable
 Oper edge port        : enable
 Admin Link type       : auto
 Oper Link type        : point-to-point
 Spanning Tree Status : enable
```

Configuring Interface Settings

You can configure RSTP attributes for specific interfaces, including port priority, path cost, link type, and edge port. You may use a different priority or path cost for ports of the same media type to indicate the preferred path, link type to indicate a point-to-point connection or shared-media connection, and edge port to indicate if the attached device can support fast forwarding.

Downloaded from www.Manualslib.com manuals search engine

Command Attributes

The following attributes are read-only and cannot be changed:

- **STA State** – Displays current state of this port within the Spanning Tree. (See Displaying Interface Settings on page 3-136 for additional information.)
  - **Discarding** - Port receives STA configuration messages, but does not forward packets.
  - **Learning** - Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses.
  - **Forwarding** - Port forwards packets, and continues learning addresses.
- **Trunk** – Indicates if a port is a member of a trunk. (STA Port Configuration only)

The following interface attributes can be configured:

- **Spanning Tree** – Enables/disables STA on this interface. (Default: Enabled).
- **Priority** – Defines the priority used for this port in the Spanning Tree Protocol. If the path cost for all ports on a switch are the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Protocol is detecting network loops. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled.
  - Default: 128
  - Range: 0-240, in steps of 16
- **Path Cost** – This parameter is used by the STP to determine the best path between devices. Therefore, lower values should be assigned to

Downloaded from www.Manualslib.com manuals search engine

ports attached to faster media, and higher values assigned to ports with slower media. (Path cost takes precedence over port priority.) Note that when the Path Cost Method is set to short (page 3-63), the maximum path cost is 65,535.

- Range –

- Ethernet: 200,000-20,000,000
- Fast Ethernet: 20,000-2,000,000
- Gigabit Ethernet: 2,000-200,000

- Default –

- Ethernet – Half duplex: 2,000,000; full duplex: 1,000,000; trunk: 500,000
- Fast Ethernet – Half duplex: 200,000; full duplex: 100,000; trunk: 50,000
- Gigabit Ethernet – Full duplex: 10,000; trunk: 5,000

- **Admin Link Type** – The link type attached to this interface.

  - Point-to-Point – A connection to exactly one other bridge.
  - Shared – A connection to two or more bridges.
  - Auto – The switch automatically determines if the interface is attached to a point-to-point link or to shared media. (This is the default setting.)

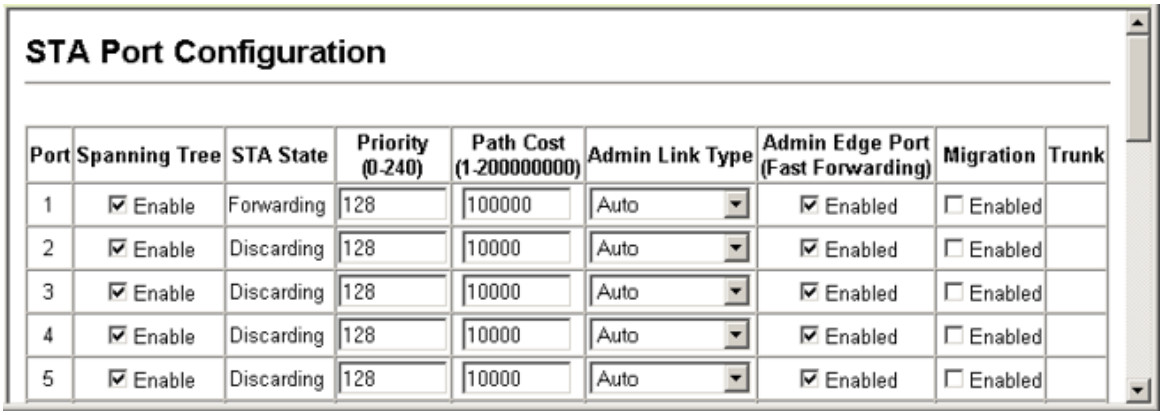
- **Admin Edge Port** (Fast Forwarding) – You can enable this option if an interface is attached to a LAN segment that is at the end of a bridged LAN or to an end node. Since end nodes **cannot** cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying Edge Ports provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to initiate reconfiguration when the interface changes state, and also overcomes other STA-related timeout problems. However, remember that Edge Port should only be enabled for ports connected to an end-node device. (Default: Disabled)

- **Migration** – If at any time the switch detects STP BPDUs, including

Downloaded from www.Manualslib.com manuals search engine

Configuration or Topology Change Notification BPDUs, it will automatically set the selected interface to forced STP-compatible mode. However, you can also use the Protocol Migration button to manually re-check the appropriate BPDU format (RSTP or STP-compatible) to send on the selected interfaces. (Default: Disabled)

Web – Click Spanning Tree, STA, Port Configuration or STA Trunk Configuration. Modify the required attributes, then click Apply.



STA Port Configuration

Port	Spanning Tree	STA State	Priority (0-240)	Path Cost (1-200000000)	Admin Link Type	Admin Edge Port (Fast Forwarding)	Migration	Trunk
1	Enable	Forwarding	128	100000	Auto	Enabled	Enabled	
2	Enable	Discarding	128	10000	Auto	Enabled	Enabled	
3	Enable	Discarding	128	10000	Auto	Enabled	Enabled	
4	Enable	Discarding	128	10000	Auto	Enabled	Enabled	
5	Enable	Discarding	128	10000	Auto	Enabled	Enabled	

CLI – This example sets STA attributes for port 7.

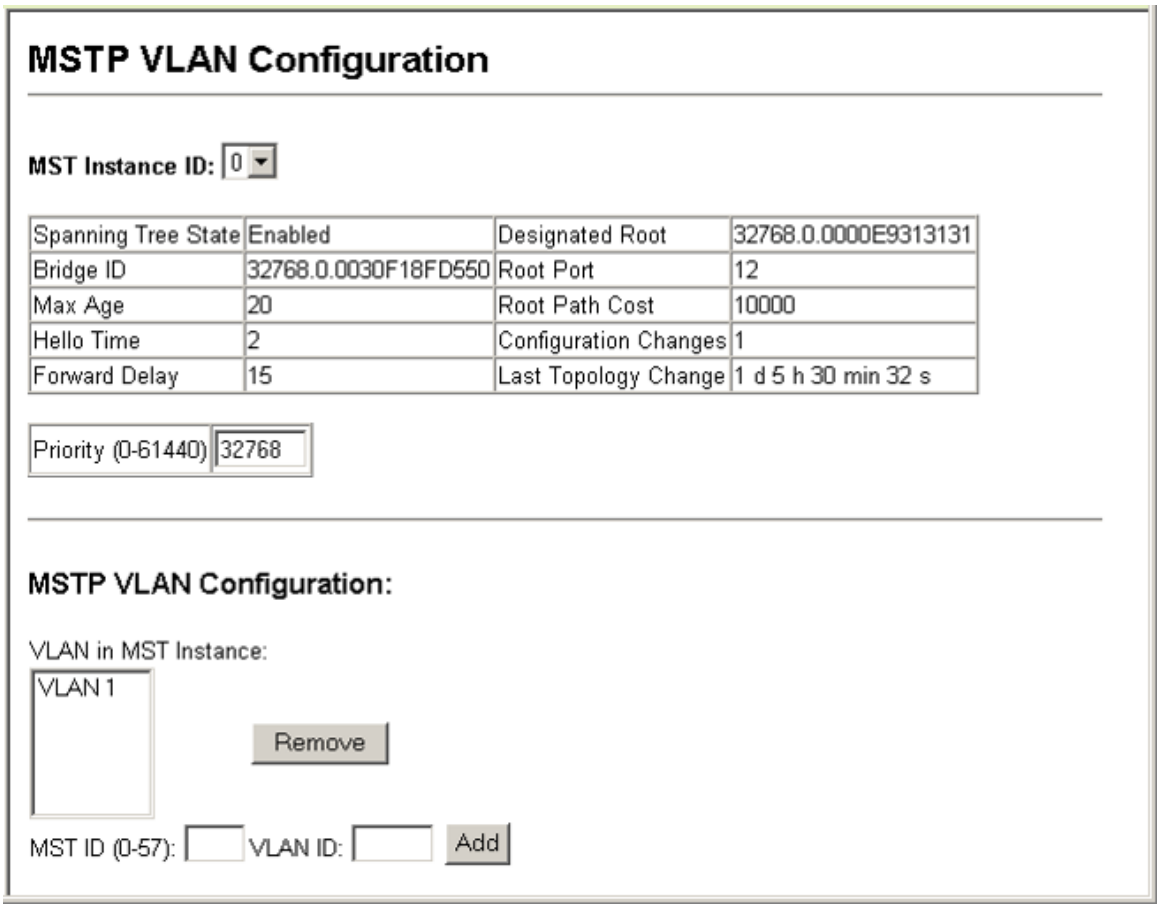
```
Console(config)#interface ethernet 1/73-1
Console(config-if)#no no spanning-tree spanning-disabled3-45
Console(config-if)#spanning-tree port-priority 03-47
Console(config-if)#spanning-tree cost 503-46
Console(config-if)#spanning-tree link-type auto3-50
Console(config-if)#no spanning-tree edge-port3-48
Console(config-if)#spanning-tree protocol-migration3-51
Console(config-if)#
```

- **VLANs in MST Instance** – VLANs assigned this instance.
- **MST ID** –
- **VLAN ID** – VLAN to assign to this selected MST instance. (Range:

Downloaded from www.Manualslib.com manuals search engine

1-4094)

Web – Click Spanning Tree, MSTP, VLAN Configuration. Select an instance identifier from the list, set the instance priority, and click Apply. To add the VLAN members to an MSTI instance, enter the instance identifier, the VLAN identifier, and click Add.



Downloaded from www.Manualslib.com manuals search engine

CLI – This displays STA settings for instance 1, followed by settings for each port.

```
Console#show spanning-tree mst 23-51
Spanning-tree information
---------------------------------------------------------------
 Spanning tree mode               :MSTP
 Spanning tree enable/disable     :enable
 Instance                         :2
 Vlans configuration              :2
 Priority                         :4096
 Bridge Hello Time (sec.)         :2
 Bridge Max Age (sec.)            :20
 Bridge Forward Delay (sec.)      :15
 Root Hello Time (sec.)           :2
 Root Max Age (sec.)              :20
 Root Forward Delay (sec.)        :15
 Max hops                         :20
 Remaining hops                   :20
 Designated Root                  :4096.2.0000E9313131
 Current root port                :0
 Current root cost                :0
 Number of topology changes       :0
 Last topology changes time (sec.):646
 Transmission limit               :3
 Path Cost Method                 :long
---------------------------------------------------------------
Eth  1/ 7 information
---------------------------------------------------------------
 Admin status         : enable
 Role                 : disable
 State                : discarding
 External path cost   : 10000
 Internal path cost   : 10000
 Priority             : 128
 Designated cost      : 0
 Designated port      : 128.7
 Designated root      : 4096.2.0000E9313131
 Designated bridge    : 4096.2.0000E9313131
 Fast forwarding      : enable
 Forward transitions  : 0
 Admin edge port      : enable
 Oper edge port       : enable
 Admin Link type      : auto
 Oper Link type       : point-to-point
 Spanning Tree Status : enable
.
.
.
```


Downloaded from www.Manualslib.com manuals search engine

CLI – This example sets the priority for MSTI 1, and adds VLANs 1-5 to this MSTI.

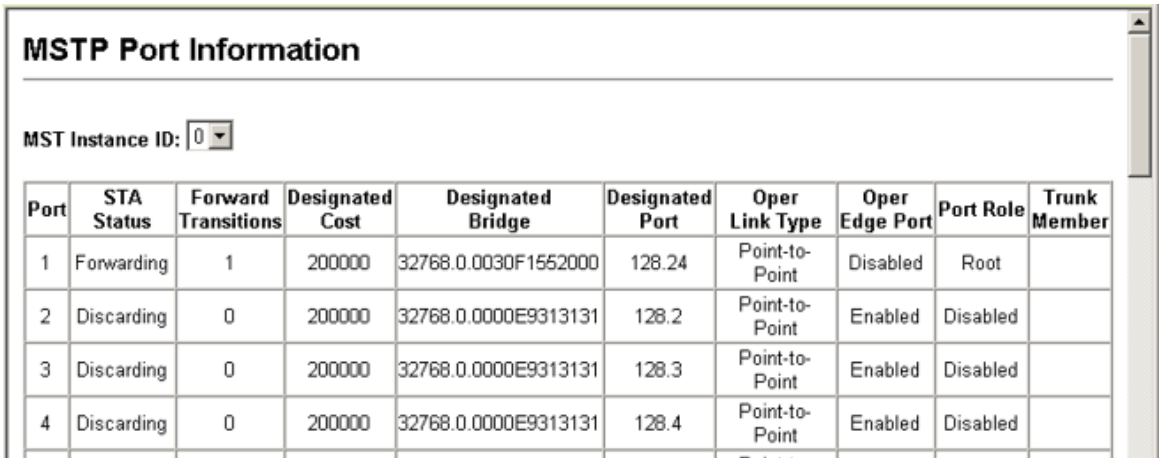
```
Console(config)#spanning-tree mst-configuration4-168
Console(config-mst)#mst 1 priority 409664-170
Console(config-mstp)#mst 1 vlan 1-54-169
Console(config-mst)#
```

Displaying Interface Settings for MSTP

The MSTP Port Information and MSTP Trunk Information pages display the current status of ports and trunks in the selected MST instance.

Field Attributes

MST Instance ID – Web – Click Spanning Tree, MSTP, Port Information or Trunk Information. Select the required MST instance to display the current spanning tree values.



MSTP Port Information

MST Instance ID: 0

Port	STA Status	Forward Transitions	Designated Cost	Designated Bridge	Designated Port	Oper Link Type	Oper Edge Port	Port Role	Trunk Member
1	Forwarding	1	200000	32768.0.0030F1552000	128.24	Point-to-Point	Disabled	Root	
2	Discarding	0	200000	32768.0.0000E9313131	128.2	Point-to-Point	Enabled	Disabled	
3	Discarding	0	200000	32768.0.0000E9313131	128.3	Point-to-Point	Enabled	Disabled	
4	Discarding	0	200000	32768.0.0000E9313131	128.4	Point-to-Point	Enabled	Disabled	

CLI – This displays STA settings for instance 0, followed by settings for each port. The settings for instance 0 are global settings that apply to the

Downloaded from www.Manualslib.com manuals search engine

IST (page 3-127), the settings for other instances only apply to the local spanning tree.

```
Console#show spanning-tree mst 03-51
Spanning-tree information
---------------------------------------------------------------
 Spanning tree mode               :MSTP
 Spanning tree enable/disable     :enable
 Instance                         :0
 Vlans configuration              :1-4094
 Priority                         :32768
 Bridge Hello Time (sec.)         :2
 Bridge Max Age (sec.)            :20
 Bridge Forward Delay (sec.)      :15
 Root Hello Time (sec.)           :2
 Root Max Age (sec.)              :20
 Root Forward Delay (sec.)        :15
 Max hops                         :20
 Remaining hops                   :20
 Designated Root                  :32768.0.0000ABCD0000
 Current root port                :1
 Current root cost                :200000
 Number of topology changes       :1
 Last topology changes time (sec.):645
 Transmission limit               :3
 Path Cost Method                 :long
---------------------------------------------------------------
Eth  1/ 1 information
---------------------------------------------------------------
 Admin status         : enable
 Role                 : root
 State                : forwarding
 External path cost   : 100000
 Internal path cost   : 100000
 Priority             : 128
 Designated cost      : 200000
 Designated port      : 128.24
 Designated root      : 32768.0.0000ABCD0000
 Designated bridge    : 32768.0.0030F1552000
 Fast forwarding      : disable
 Forward transitions  : 1
 Admin edge port      : enable
 Oper edge port       : disable
 Admin Link type      : auto
 Oper Link type       : point-to-point
 Spanning Tree Status : enable
.
.
.
```


Downloaded from www.Manualslib.com manuals search engine

Configuring Interface Settings for MSTP

You can configure the STA interface settings for an MST Instance using the MSTP Port Configuration and MSTP Trunk Configuration pages.

Field Attributes

The following attributes are read-only and cannot be changed:

- **STA State** – Displays current state of this port within the Spanning Tree. (See Displaying Interface Settings on page 3-136 for additional information.)
    - **Discarding** - Port receives STA configuration messages, but does not forward packets.
    - **Learning** - Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses.
    - **Forwarding** - Port forwards packets, and continues learning addresses.
- **Trunk** – Indicates if a port is a member of a trunk. (STA Port Configuration only)

The following interface attributes can be configured:

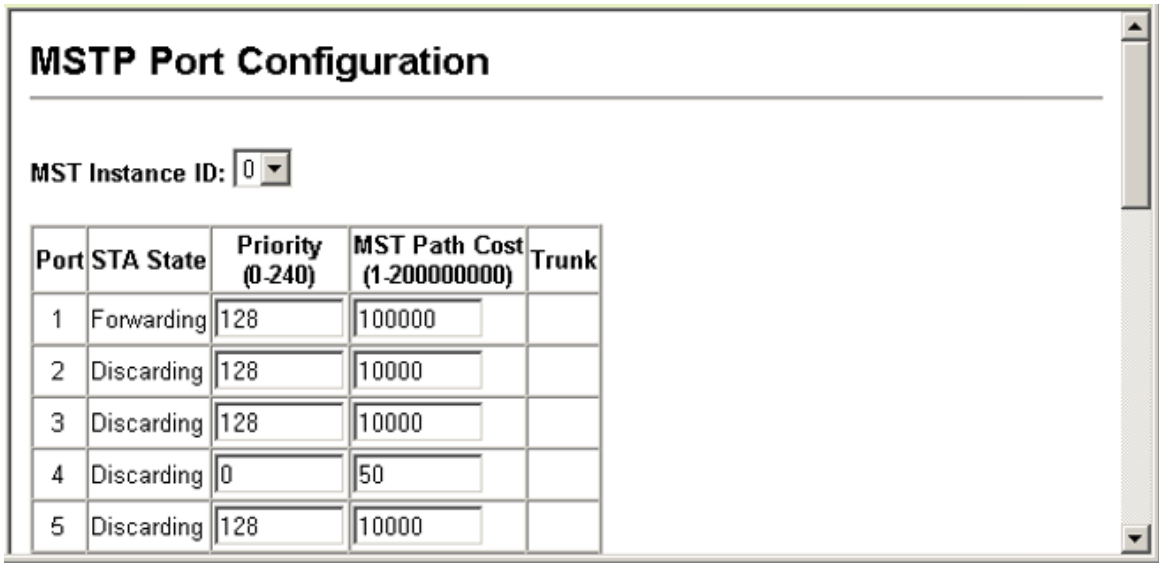
- **MST Instance ID – Priority** – Defines the priority used for this port in the Spanning Tree Protocol. If the path cost for all ports on a switch are the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Protocol is detecting network loops. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled.
    - Default: 128
    - Range: 0-240, in steps of 16
- **MST Path Cost** – This parameter is used by the MSTP to determine

Downloaded from www.Manualslib.com manuals search engine

the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. (Path cost takes precedence over port priority.) Note that when the Path Cost Method is set to short (page 3-63), the maximum path cost is 65,535.

- Range –
  - Ethernet: 200,000-20,000,000
  - Fast Ethernet: 20,000-2,000,000
  - Gigabit Ethernet: 2,000-200,000
- Default –
  - Ethernet – Half duplex: 2,000,000; full duplex: 1,000,000; trunk: 500,000
  - Fast Ethernet – Half duplex: 200,000; full duplex: 100,000; trunk: 50,000
  - Gigabit Ethernet – Full duplex: 10,000; trunk: 5,000

Web – Click Spanning Tree, MSTP, Port Configuration or Trunk Configuration. Enter the priority and path cost for an interface, and click Apply.


MSTP Port Configuration
MST Instance ID: 0
Port STA State Priority (0-240) MST Path Cost (1-200000000) Trunk
1 Forwarding 128 100000
2 Discarding 128 10000
3 Discarding 128 10000
4 Discarding 0 50
5 Discarding 128 10000

CLI – This example sets the MSTP attributes for port 4.

```
Console(config)#interface ethernet 1/43-1
Console(config-if)#spanning-tree mst port-priority 04-177
Console(config-if)#spanning-tree mst cost 504-176
Console(config-if)
```


Downloaded from www.Manualslib.com manuals search engine

VLAN Configuration

Overview

In large networks, routers are used to isolate broadcast traffic for each subnet into separate domains. This switch provides a similar service at Layer 2 by using VLANs to organize any group of network nodes into separate broadcast domains. VLANs confine broadcast traffic to the originating group, and can eliminate broadcast storms in large networks. This also provides a more secure and cleaner network environment.

An IEEE 802.1Q VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment.

VLANs help to simplify network management by allowing you to move devices to a new VLAN without having to change any physical connections. VLANs can be easily organized to reflect departmental groups (such as Marketing or R&D), usage groups (such as e-mail), or multicast groups (used for multimedia applications such as videoconferencing).

VLANs provide greater network efficiency by reducing broadcast traffic, and allow you to make network changes without having to update IP addresses or IP subnets. VLANs inherently provide a high level of network security since traffic must pass through a configured Layer 3 link to reach a different VLAN.

This switch supports the following VLAN features:

- Up to 255 VLANs based on the IEEE 802.1Q standard
- Distributed VLAN learning across multiple switches using explicit or implicit tagging and GVRP protocol
- Port overlapping, allowing a port to participate in multiple VLANs
- End stations can belong to multiple VLANs
- Passing traffic between VLAN-aware and VLAN-unaware devices

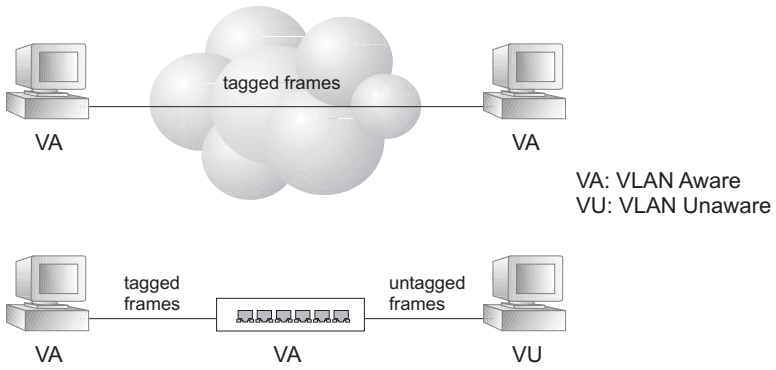
Downloaded from www.Manualslib.com manuals search engine

- Priority tagging

Assigning Ports to VLANs

Before enabling VLANs for the switch, you must first assign each port to the VLAN group(s) in which it will participate. By default all ports are assigned to VLAN 1 as untagged ports. Add a port as a tagged port if you want it to carry traffic for one or more VLANs, and any intermediate network devices or the host at the other end of the connection supports VLANs. Then assign ports on the other VLAN-aware network devices along the path that will carry this traffic to the same VLAN(s), either manually or dynamically using GVRP. However, if you want a port on this switch to participate in one or more VLANs, but none of the intermediate network devices nor the host at the other end of the connection supports VLANs, then you should add this port to the VLAN as an untagged port.

Note: VLAN-tagged frames can pass through VLAN-aware or VLAN-unaware network interconnection devices, but the VLAN tags should be stripped off before passing it on to any end-node host that does not support VLAN tagging.



VLAN Classification – When the switch receives a frame, it classifies the frame in one of two ways. If the frame is untagged, the switch assigns the frame to an associated VLAN (based on the default VLAN ID of the receiving port). But if the frame is tagged, the switch uses the tagged VLAN ID to identify the port broadcast domain of the frame.

Downloaded from www.Manualslib.com manuals search engine

Port Overlapping – Port overlapping can be used to allow access to commonly shared network resources among different VLAN groups, such as file servers or printers. Note that if you implement VLANs which do not overlap, but still need to communicate, you can connect them by enabled routing on this switch.

Untagged VLANs – Untagged (or static) VLANs are typically used to reduce broadcast traffic and to increase security. A group of network users assigned to a VLAN form a broadcast domain that is separate from other VLANs configured on the switch. Packets are forwarded only between ports that are designated for the same VLAN. Untagged VLANs can be used to manually isolate user groups or subnets. However, you should use IEEE 802.3 tagged VLANs with GVRP whenever possible to fully automate VLAN registration.

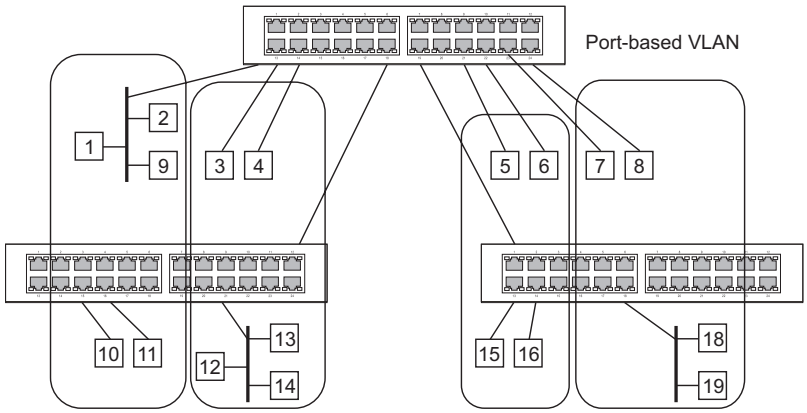
Automatic VLAN Registration – GVRP (GARP VLAN Registration Protocol) defines a system whereby the switch can automatically learn the VLANs to which each end station should be assigned. If an end station (or its network adapter) supports the IEEE 802.1Q VLAN protocol, it can be configured to broadcast a message to your network indicating the VLAN groups it wants to join. When this switch receives these messages, it will automatically place the receiving port in the specified VLANs, and then forward the message to all other ports. When the message arrives at another switch that supports GVRP, it will also place the receiving port in the specified VLANs, and pass the message on to all other ports. VLAN requirements are propagated in this way throughout the network. This allows GVRP-compliant devices to be automatically configured for VLAN groups based solely on endstation requests.

To implement GVRP in a network, first add the host devices to the required VLANs (using the operating system or other application software), so that these VLANs can be propagated onto the network. For both the edge switches attached directly to these hosts, and core switches in the network, enable GVRP on the links between these devices. You should also determine security boundaries in the network and disable

Downloaded from www.Manualslib.com manuals search engine

GVRP on the boundary ports to prevent advertisements from being propagated, or forbid those ports from joining restricted VLANs.

Note: If you have host devices that do not support GVRP, you should configure static or untagged VLANs for the switch ports connected to these devices (as described in "Adding Static Members to VLANs (VLAN Index)" on page 3-159). But you can still enable GVRP on these edge switches, as well as on the core switches in the network.



Forwarding Tagged/Untagged Frames

If you want to create a small port-based VLAN for devices attached directly to a single switch, you can assign ports to the same untagged VLAN. However, to participate in a VLAN group that crosses several switches, you should create a VLAN for that group and enable tagging on all ports.

Ports can be assigned to multiple tagged or untagged VLANs. Each port on the switch is therefore capable of passing tagged or untagged frames. When forwarding a frame from this switch along a path that contains any VLAN-aware devices, the switch should include VLAN tags. When forwarding a frame from this switch along a path that does not contain any VLAN-aware devices (including the destination host), the switch must first strip off the VLAN tag before forwarding the frame. When the switch receives a tagged frame, it will pass this frame onto the VLAN(s) indicated by the frame tag. However, when this switch receives an untagged frame

Downloaded from www.Manualslib.com manuals search engine

from a VLAN-unaware device, it first decides where to forward the frame, and then inserts a VLAN tag reflecting the ingress port's default VID.

Enabling or Disabling GVRP (Global Setting)

GARP VLAN Registration Protocol (GVRP) defines a way for switches to exchange VLAN information in order to register VLAN members on ports across the network. VLANs are dynamically configured based on join messages issued by host devices and propagated throughout the network. GVRP must be enabled to permit automatic VLAN registration, and to support VLANs which extend beyond the local switch. (Default: Disabled)

Web – Click VLAN, 802.1Q VLAN, GVRP Status. Enable or disable GVRP, click Apply

CLI – This example enables GVRP for the switch.

```
Console(config)#bridge-ext gvrp3-72
Console(config)#
```

Displaying Basic VLAN Information

The VLAN Basic Information page displays basic information on the VLAN type supported by the switch.

Field Attributes

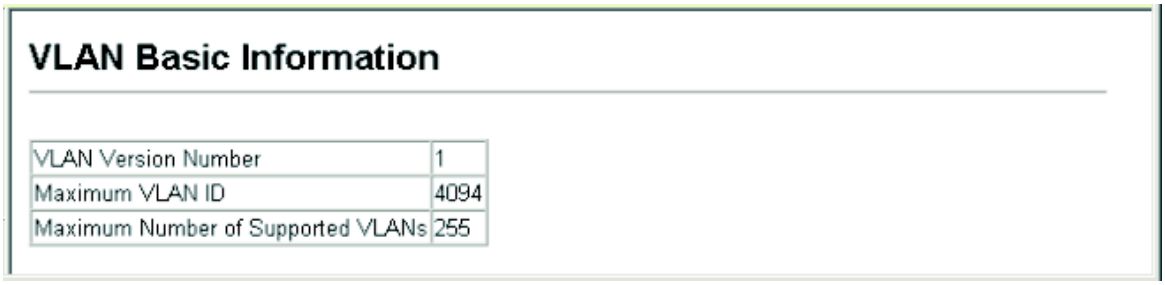
- **VLAN Version Number*** – The VLAN version used by this switch as specified in the IEEE 802.1Q standard.
- **Maximum VLAN ID** – Maximum VLAN ID recognized by this switch.
- **Maximum Number of Supported VLANs** – Maximum number of

Downloaded from www.Manualslib.com manuals search engine

VLANs that can be configured on this switch.

* Web Only

Web – Click VLAN, 802.1Q VLAN, Basic Information.



VLAN Basic Information

VLAN Version Number	1
Maximum VLAN ID	4094
Maximum Number of Supported VLANs	255

CLI – Enter the following command.

```
Console#show bridge-ext3-73
 Max support vlan numbers: 255
 Max support vlan ID: 4094
 Extended multicast filtering services: No
 Static entry individual port: Yes
 VLAN learning: IVL
 Configurable PVID tagging: Yes
 Local VLAN capable: Yes
 Traffic classes: Enabled
 Global GVRP status: Disabled
 GMRP: Disabled
Console#
```

Displaying Current VLANs

The VLAN Current Table shows the current port members of each VLAN and whether or not the port supports VLAN tagging. Ports assigned to a large VLAN group that crosses several switches should use VLAN tagging. However, if you just want to create a small port-based VLAN for one or two switches, you can disable tagging.

Command Attributes (Web)

- **VLAN ID** – ID of configured VLAN (1-4094).
- **Up Time at Creation** – Time this VLAN was created (i.e., System Up Time).
- **Status** – Shows how this VLAN was added to the switch.
  - **Dynamic GVRP**: Automatically learned via GVRP.

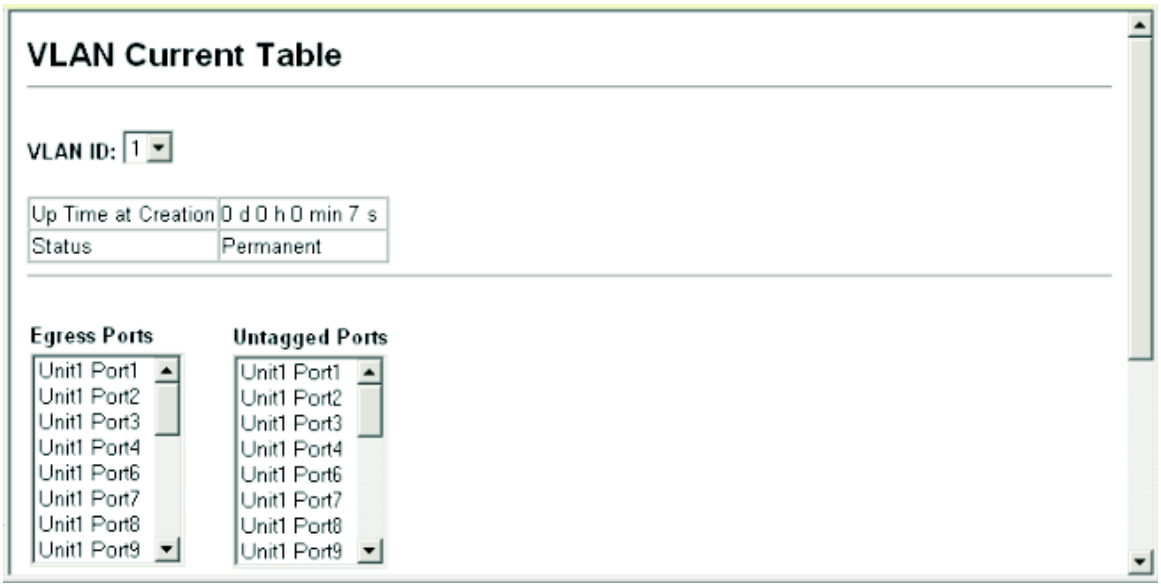
Downloaded from www.Manualslib.com manuals search engine

- **Permanent**: Added as a static entry.

- **Egress Ports** – Shows all the VLAN port members.

- **Untagged Ports** – Shows the untagged VLAN port members.

Web – Click VLAN, 802.1Q VLAN, Current Table. Select any ID from the scroll-down list.



Command Attributes (CLI)

- **VLAN** – ID of configured VLAN (1-4094, no leading zeroes).

- **Type** – Shows how this VLAN was added to the switch.
  - **Dynamic**: Automatically learned via GVRP.
  - **Static**: Added as a static entry.

- **Name** – Name of the VLAN (1 to 32 characters).

- **Status** – Shows if this VLAN is enabled or disabled.
  - **Active**: VLAN is operational.
  - **Suspend**: VLAN is suspended; i.e., does not pass packets.

- **Ports / Channel groups** – Shows the VLAN interface members.

Downloaded from www.Manualslib.com manuals search engine

CLI – Current VLAN information can be displayed with the following command.

```
Console#show vlan id 1-64
VLAN Type    Name         Status   Ports/Channel groups
---- ------- ----------- ------   -----------------------------------
1    Static  DefaultVlan  Active Eth1/1  Eth1/2  Eth1/3  Eth1/4  Eth1/5
                                 Eth1/6  Eth1/7  Eth1/8  Eth1/9  Eth1/10
                                 Eth1/11 Eth1/12

Console#
```


Downloaded from www.Manualslib.com manuals search engine

Creating VLANs

Use the VLAN Static List to create or remove VLAN groups. To propagate information about VLAN groups used on this switch to external network devices, you must specify a VLAN ID for each of these groups.

Command Attributes

- **Current** – Lists all the current VLAN groups created for this system. Up to 255 VLAN groups can be defined. VLAN 1 is the default untagged VLAN.

- **New** – Allows you to specify the name and numeric identifier for a new VLAN group. (The VLAN name is only used for management on this system; it is not added to the VLAN tag.)

- **VLAN ID** – ID of configured VLAN (1-4094, no leading zeroes).

- **VLAN Name** – Name of the VLAN (1 to 32 characters).

- **Status** (Web) – Enables or disables the specified VLAN.
  - **Enable**: VLAN is operational.
  - **Disable**: VLAN is suspended; i.e., does not pass packets.

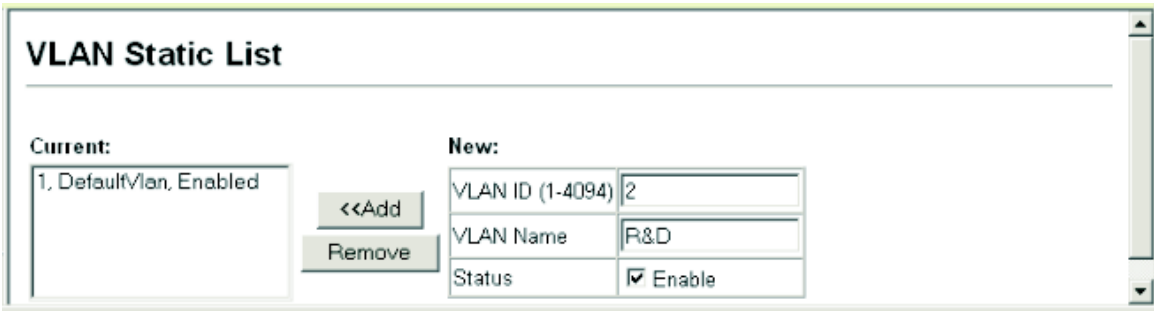
- **State** (CLI) – Enables or disables the specified VLAN.
  - **Active**: VLAN is operational.
  - **Suspend**: VLAN is suspended; i.e., does not pass packets.

- **Add** – Adds a new VLAN group to the current list.

- **Remove** – Removes a VLAN group from the current list. If any port is assigned to this group as untagged, it will be reassigned to VLAN group 1 as untagged.

Web – Click VLAN, 802.1Q VLAN, Static List. To create a new VLAN, enter the VLAN ID and VLAN name, mark the Enable checkbox to activate the VLAN, and then click Add.

Downloaded from www.Manualslib.com manuals search engine



CLI – This example creates a new VLAN.

```
Console(config)#vlan database3-54
Console(config-vlan)#vlan 2 name R&D media ethernet state active3-55
Console(config-vlan)#end
Console#show vlan3-64
VLAN Type    Name              Status    Ports/Channel groups
---- ------- ----------------- --------- ---------------------------------
   1  Static     DefaultVlan    Active Eth1/ 1 Eth1/ 2 Eth1/ 3 Eth1/ 4 Eth1/ 5
                                      Eth1/ 6 Eth1/ 7 Eth1/ 8 Eth1/ 9 Eth1/10
                                          Eth1/11 Eth1/12
   2  Static              R&D    Active
Console(config-vlan)#
```

Adding Static Members to VLANs (VLAN Index)

Use the VLAN Static Table to configure port members for the selected VLAN index. Assign ports as tagged if they are connected to 802.1Q VLAN compliant devices, or untagged they are not connected to any VLAN-aware devices. Or configure a port as forbidden to prevent the switch from automatically adding it to a VLAN via the GVRP protocol.

Notes: **1.** You can also use the VLAN Static Membership by Port page to configure VLAN groups based on the port index (page 3-161). However, note that this configuration page can only add ports to a VLAN as tagged members.

2. VLAN 1 is the default untagged VLAN containing all ports on the switch, and can only be modified by first reassigning the default port VLAN ID as described under "Configuring VLAN Behavior for Interfaces" on page 3-163.

Command Attributes

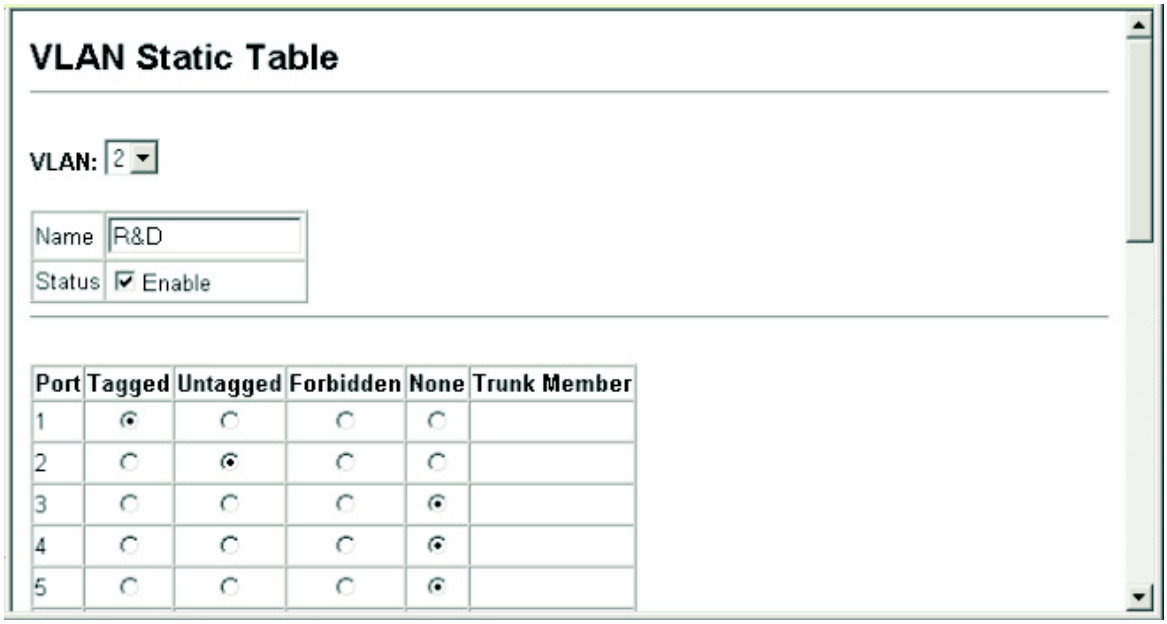
- **VLAN** – ID of configured VLAN (1-4094, no leading zeroes).

Downloaded from www.Manualslib.com manuals search engine

- **Name** – Name of the VLAN (1 to 32 characters).
- **Status** – Enables or disables the specified VLAN.
  - **Enable**: VLAN is operational.
  - **Disable**: VLAN is suspended; i.e., does not pass packets.
- **Port** – Port identifier.
- **Trunk** – Trunk identifier.
- **Membership Type** – Select VLAN membership for each interface by marking the appropriate radio button for a port or trunk:
  - **Tagged**: Interface is a member of the VLAN. All packets transmitted by the port will be tagged, that is, carry a tag and therefore carry VLAN or CoS information.
  - **Untagged**: Interface is a member of the VLAN. All packets transmitted by the port will be untagged, that is, not carry a tag and therefore not carry VLAN or CoS information. Note that an interface must be assigned to at least one group as an untagged port.
  - **Forbidden**: Interface is forbidden from automatically joining the VLAN via GVRP. For more information, see "Automatic VLAN Registration" on page 3-152.
  - **None**: Interface is not a member of the VLAN. Packets associated with this VLAN will not be transmitted by the interface.
- **Trunk Member** – Indicates if a port is a member of a trunk. To add a trunk to the selected VLAN, use the last table on the VLAN Static Table page.

Downloaded from www.Manualslib.com manuals search engine

Web – Click VLAN, 802.1Q VLAN, Static Table. Select a VLAN ID from the scroll-down list. Modify the VLAN name and status if required. Select the membership type by marking the appropriate radio button in the list of ports or trunks. Click Apply.



CLI – The following example adds tagged and untagged ports to VLAN 2.

```
Console(config)#interface ethernet 1/13-1
Console(config-if)#switchport allowed vlan add 2 tagged3-62
Console(config-if)#exit
Console(config)#interface ethernet 1/2
Console(config-if)#switchport allowed vlan add 2 untagged
Console(config-if)#exit
Console(config)#interface ethernet 1/13
Console(config-if)#switchport allowed vlan add 2 tagged
```

Adding Static Members to VLANs (Port Index)

Use the VLAN Static Membership by Port menu to assign VLAN groups to the selected interface as a tagged member.

Command Attributes

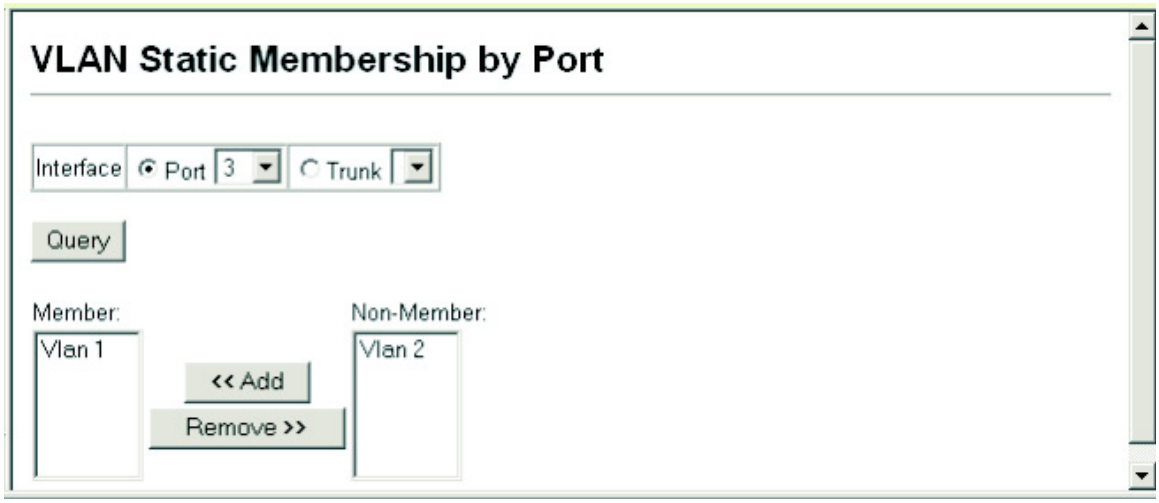
- **Interface** – Port or trunk identifier.
- **Member** – VLANs for which the selected interface is a tagged member.

Downloaded from www.Manualslib.com manuals search engine

- **Non-Member** – VLANs for which the selected interface is not a tagged member.

Downloaded from www.Manualslib.com manuals search engine

Web – Open VLAN, 802.1Q VLAN, Static Membership. Select an interface from the scroll-down box (Port or Trunk). Click Query to display membership information for the interface. Select a VLAN ID, and then click Add to add the interface as a tagged member, or click Remove to remove the interface. After configuring VLAN membership for each interface, click Apply.



CLI – This example adds Port 3 to VLAN 1 as a tagged port, and removes Port 3 from VLAN 2.

```
Console(config)#interface ethernet 1/33-1
Console(config-if)#switchport allowed vlan add 1 tagged3-62
Console(config-if)#switchport allowed vlan remove 2
```

Configuring VLAN Behavior for Interfaces

You can configure VLAN behavior for specific interfaces, including the default VLAN identifier (PVID), accepted frame types, ingress filtering, GVRP status, and GARP timers.

Command Usage

- **GVRP** – GARP VLAN Registration Protocol defines a way for switches to exchange VLAN information in order to automatically register VLAN members on interfaces across the network.
- **GARP** – Group Address Registration Protocol is used by GVRP to register or deregister client attributes for client services within a

Downloaded from www.Manualslib.com manuals search engine

bridged LAN. The default values for the GARP timers are independent of the media access method or data rate. These values should not be changed unless you are experiencing difficulties with GVRP registration/deregistration.

Command Attributes

- **PVID** – VLAN ID assigned to untagged frames received on the interface. (Default: 1)

  - If an interface is not a member of VLAN 1 and you assign its PVID to this VLAN, the interface will automatically be added to VLAN 1 as an untagged member. For all other VLANs, an interface must first be configured as an untagged member before you can assign its PVID to that group.

- **Acceptable Frame Type** – Sets the interface to accept all frame types, including tagged or untagged frames, or only tagged frames. When set to receive all frame types, any received frames that are untagged are assigned to the default VLAN. (Option: All, Tagged; Default: All)

- **Ingress Filtering** – Determines how to process frames tagged for VLANs for which the ingress port is not a member. (Default: Disabled)

  - Ingress filtering only affects tagged frames.
  - If ingress filtering is disabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be flooded to all other ports (except for those VLANs explicitly forbidden on this port).
  - If ingress filtering is enabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be discarded.
  - Ingress filtering does not affect VLAN independent BPDU frames, such as GVRP or STP. However, they do affect VLAN dependent BPDU frames, such as GMRP.

- **GVRP Status** – Enables/disables GVRP for the interface. GVRP

Downloaded from www.Manualslib.com manuals search engine

must be globally enabled for the switch before this setting can take effect. (See "Displaying Bridge Extension Capabilities" on page 3-18.) When disabled, any GVRP packets received on this port will be discarded and no GVRP registrations will be propagated from other ports. (Default: Disabled)

- **GARP Join Timer*** – The interval between transmitting requests/ queries to participate in a VLAN group. (Range: 20-1000 centiseconds; Default: 20)

- **GARP Leave Timer*** – The interval a port waits before leaving a VLAN group. This time should be set to more than twice the join time. This ensures that after a Leave or LeaveAll message has been issued, the applicants can rejoin before the port actually leaves the group. (Range: 60-3000 centiseconds; Default: 60)

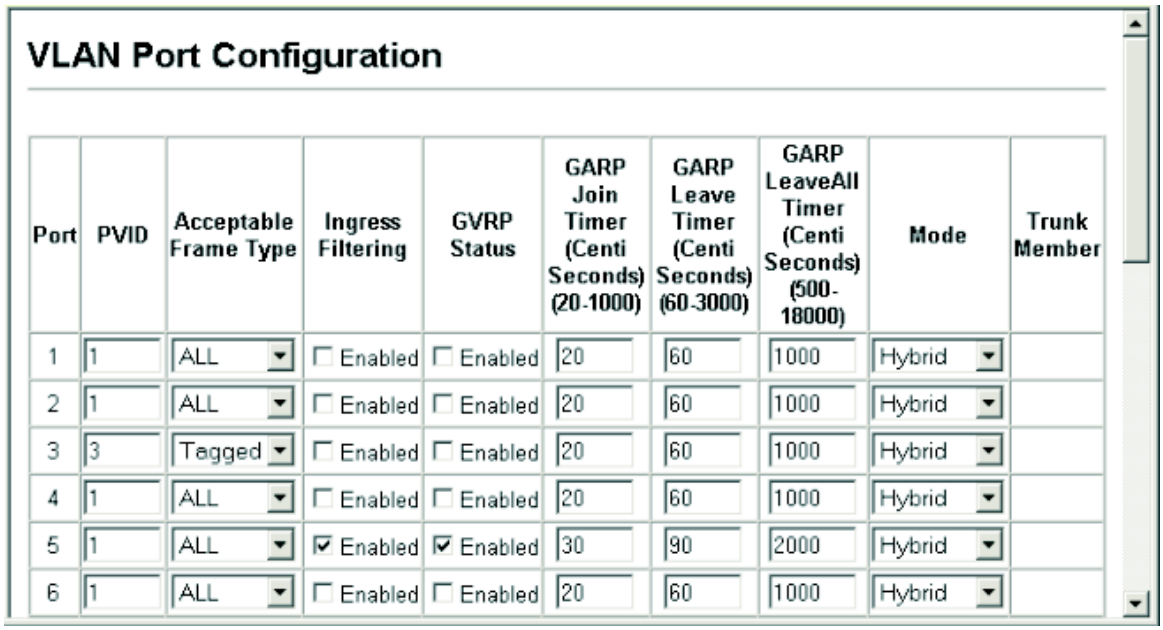
- **GARP LeaveAll Timer*** – The interval between sending out a LeaveAll query message for VLAN group participants and the port leaving the group. This interval should be considerably larger than the Leave Time to minimize the amount of traffic generated by nodes rejoining the group.
(Range: 500-18000 centiseconds; Default: 1000)

- **Mode** – Indicates VLAN membership mode for an interface. (Default: 1Q Trunk)
  - **1Q Trunk** – Specifies a port as an end-point for a VLAN trunk. A trunk is a direct link between two switches, so the port transmits tagged frames that identify the source VLAN. However, note that frames belonging to the port's default VLAN (i.e., associated with the PVID) are sent untagged.
  - **Hybrid** – Specifies a hybrid VLAN interface. The port may transmit tagged or untagged frames.
- **Trunk Member** – Indicates if a port is a member of a trunk. To add a trunk to the selected VLAN, use the last table on the VLAN Static Table page.

Downloaded from www.Manualslib.com manuals search engine

* Timer settings must follow this rule: 2 x (join timer) < leave timer < leaveAll timer

Web – Click VLAN, 802.1Q VLAN, Port Configuration or VLAN Trunk Configuration. Fill in the required settings for each interface, click Apply.



VLAN Port Configuration

Port	PVID	Acceptable Frame Type	Ingress Filtering	GVRP Status	GARP Join Timer (Centi Seconds) (20-1000)	GARP Leave Timer (Centi Seconds) (60-3000)	GARP LeaveAll Timer (Centi Seconds) (500-18000)	Mode	Trunk Member
1	1	ALL	Enabled	Enabled	20	60	1000	Hybrid	
2	1	ALL	Enabled	Enabled	20	60	1000	Hybrid	
3	3	Tagged	Enabled	Enabled	20	60	1000	Hybrid	
4	1	ALL	Enabled	Enabled	20	60	1000	Hybrid	
5	1	ALL	Enabled	Enabled	30	90	2000	Hybrid	
6	1	ALL	Enabled	Enabled	20	60	1000	Hybrid	

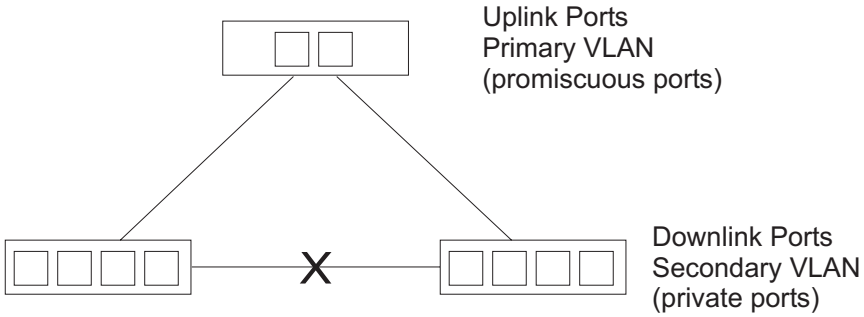
CLI – This example sets port 3 to accept only tagged frames, assigns PVID 3 as the native VLAN ID, enables GVRP, sets the GARP timers, and then sets the switchport mode to hybrid.

```
Console(config)#interface ethernet 1/3 3-1
Console(config-if)#switchport acceptable-frame-types tagged 3-59
Console(config-if)#switchport ingress-filtering 3-60
Console(config-if)#switchport native vlan 3 3-61
Console(config-if)#switchport gvrp 3-73
Console(config-if)#garp timer join 20 3-75
Console(config-if)#garp timer leave 90
Console(config-if)#garp timer leaveall 2000
Console(config-if)#switchport mode hybrid 3-58
Console(config-if)#
```


Downloaded from www.Manualslib.com manuals search engine

Configuring Private VLANs

Private VLANs provide port-based security and isolation between ports within the assigned VLAN. Data traffic on downlink ports can only be forwarded to, and from, uplink ports. (Note that private VLANs and normal VLANs can exist simultaneously within the same switch.)



Enabling Private VLANs

Use the Private VLAN Status page to enable/disable the Private VLAN function.

Web – Click VLAN, Private VLAN, Status. Select Enable or Disable from the scroll-down box, and click Apply.

CLI – This example enables private VLANs.

```
Console(config)#pvlan3-70
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

Configuring Uplink and Downlink Ports

Use the Private VLAN Link Status page to set ports as downlink or uplink ports. Ports designated as downlink ports can not communicate with any other ports on the switch except for the uplink ports. Uplink ports can communicate with any other ports on the switch and with any designated downlink ports.

Web – Click VLAN, Private VLAN, Link Status. Mark the ports that will serve as uplinks and downlinks for the private VLAN, then click Apply.

CLI – This configures ports 3 and 4 as uplinks and ports 5 and 6 as downlinks.

```
Console(config)#pvlan uplink 1/3-4 downlink 1/5-63-70
Console(config)#
```

Configuring Protocol-Based VLANs

The network devices required to support multiple protocols cannot be easily grouped into a common VLAN. This may require non-standard devices to pass traffic between different VLANs in order to encompass all the devices participating in a specific protocol. This kind of configuration deprives users of the basic benefits of VLANs, including security and easy accessibility.

To avoid these problems, you can configure this switch with protocol-based VLANs that divide the physical network into logical VLAN groups for each required protocol. When a frame is received at a

Downloaded from www.Manualslib.com manuals search engine

port, its VLAN membership can then be determined based on the protocol type being used by the inbound packets.

Command Usage

To configure protocol-based VLANs, follow these steps:

1. First configure VLAN groups for the protocols you want to use (page 3-158). Although not mandatory, we suggest configuring a separate VLAN for each major protocol running on your network. Do not add port members at this time.
2. Create a protocol group for each of the protocols you want to assign to a VLAN using the Protocol VLAN Configuration page.
3. Then map the protocol for each interface to the appropriate VLAN using the Protocol VLAN Port Configuration page.

Configuring Protocol Groups

Create a protocol group for one or more protocols.

Command Attributes

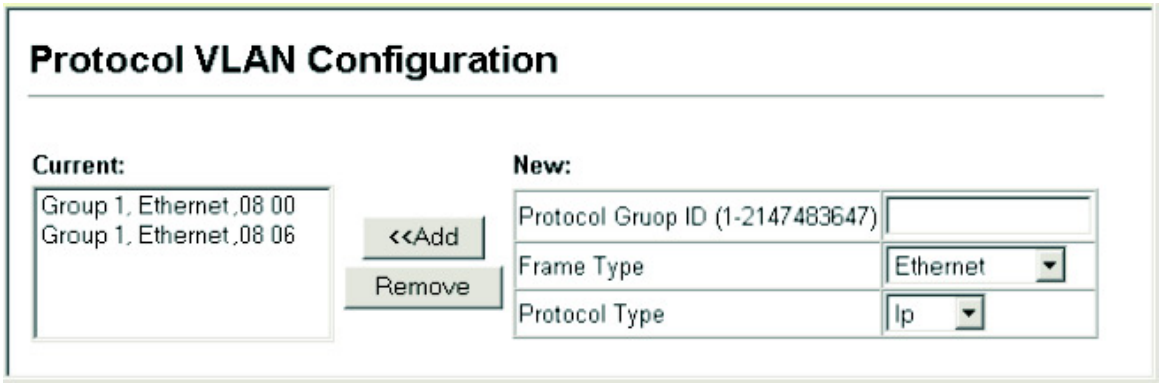
- **Protocol Group ID** – Group identifier of this protocol group. (Range: 1-2147483647)

- **Frame Type** – Frame type used by this protocol. (Options: Ethernet, RFC_1042, SNAP_8021h, SNAP_other, LLC_other)

- **Protocol Type** – The only option for the LLC_other frame type is IPX_raw. The options for all other frames types include: IP, ARP, RARP.

Web – Click VLAN, Protocol VLAN, Configuration. Enter a protocol group ID, frame type and protocol type, then click Apply.

Downloaded from www.Manualslib.com manuals search engine



CLI – The following creates protocol group 1, and then specifies Ethernet frames with IP and ARP protocol types.

```
Console(config)#protocol-vlan protocol-group 1
add frame-type ethernet protocol-type ip3-66
Console(config)#protocol-vlan protocol-group 1
add frame-type ethernet protocol-type arp
Console(config)#
```

Mapping Protocols to VLANs

Map a protocol group to a VLAN for each interface that will participate in the group.

Command Usage

- When creating a protocol-based VLAN, only assign interfaces using this configuration screen. If you assign interfaces using any of the other VLAN commands such as VLAN Static Table (page 3-159) or VLAN Static Membership (page 3-161), these interfaces will admit traffic of any protocol type into the associated VLAN.

- When a frame enters a port that has been assigned to a protocol VLAN, it is processed in the following manner:

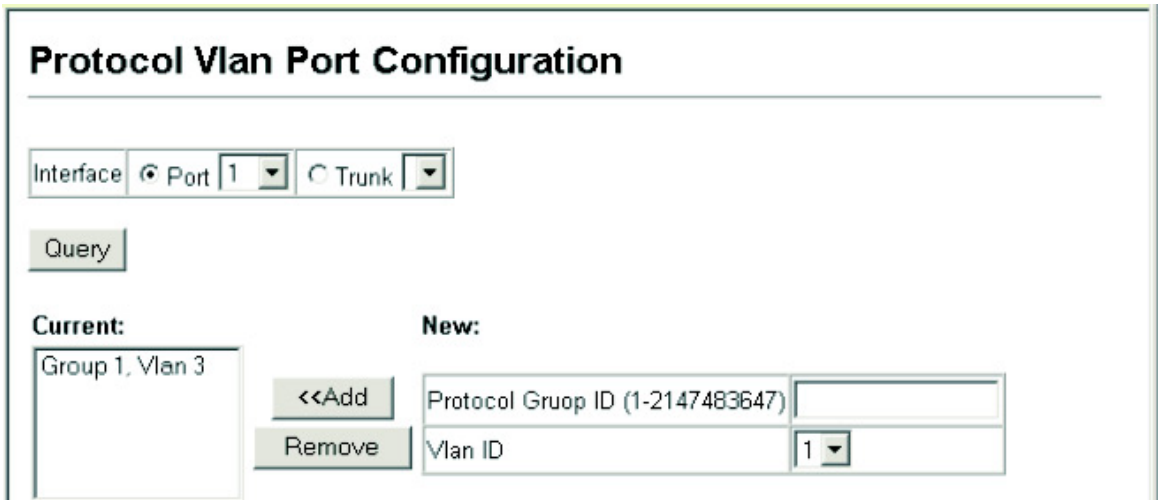
  - If the frame is tagged, it will be processed according to the standard rules applied to tagged frames.
  - If the frame is untagged and the protocol type matches, the frame is forwarded to the appropriate VLAN.
  - If the frame is untagged but the protocol type does not match, the frame is forwarded to the default VLAN for this interface.

Downloaded from www.Manualslib.com manuals search engine

Command Attributes

- **Interface** – Port or trunk identifier.
- **Protocol Group ID** – Group identifier of this protocol group. (Range: 1-2147483647)
- **VLAN ID** – VLAN to which matching protocol traffic is forwarded. (Range: 1-4094)

Web – Click VLAN, Protocol VLAN, Port Configuration. Select a a port or trunk, enter a protocol group ID, the corresponding VLAN ID, and click Apply.



CLI – The following maps the traffic entering Port 1 which matches the protocol type specified in protocol group 1 to VLAN 3.

```
Console(config)#interface ethernet 1/1
Console(config-if)#protocol-vlan protocol-group 1 vlan 33-67
Console(config-if)#
```


Downloaded from www.Manualslib.com manuals search engine

Class of Service Configuration

Class of Service (CoS) allows you to specify which data packets have greater precedence when traffic is buffered in the switch due to congestion. This switch supports CoS with eight priority queues for each port. Data packets in a port's high-priority queue will be transmitted before those in the lower-priority queues. You can set the default priority for each interface, and configure the mapping of frame priority tags to the switch's priority queues.

Setting the Default Priority for Interfaces

You can specify the default port priority for each interface on the switch. All untagged packets entering the switch are tagged with the specified default port priority, and then sorted into the appropriate priority queue at the output port.

Command Usage

- This switch provides eight priority queues for each port. It uses Weighted Round Robin to prevent head-of-queue blockage.
- The default priority applies for an untagged frame received on a port set to accept all frame types (i.e, receives both untagged and tagged frames). This priority does not apply to IEEE 802.1Q VLAN tagged frames. If the incoming frame is an IEEE 802.1Q VLAN tagged frame, the IEEE 802.1p User Priority bits will be used.
- If the output port is an untagged member of the associated VLAN, these frames are stripped of all VLAN tags prior to transmission.

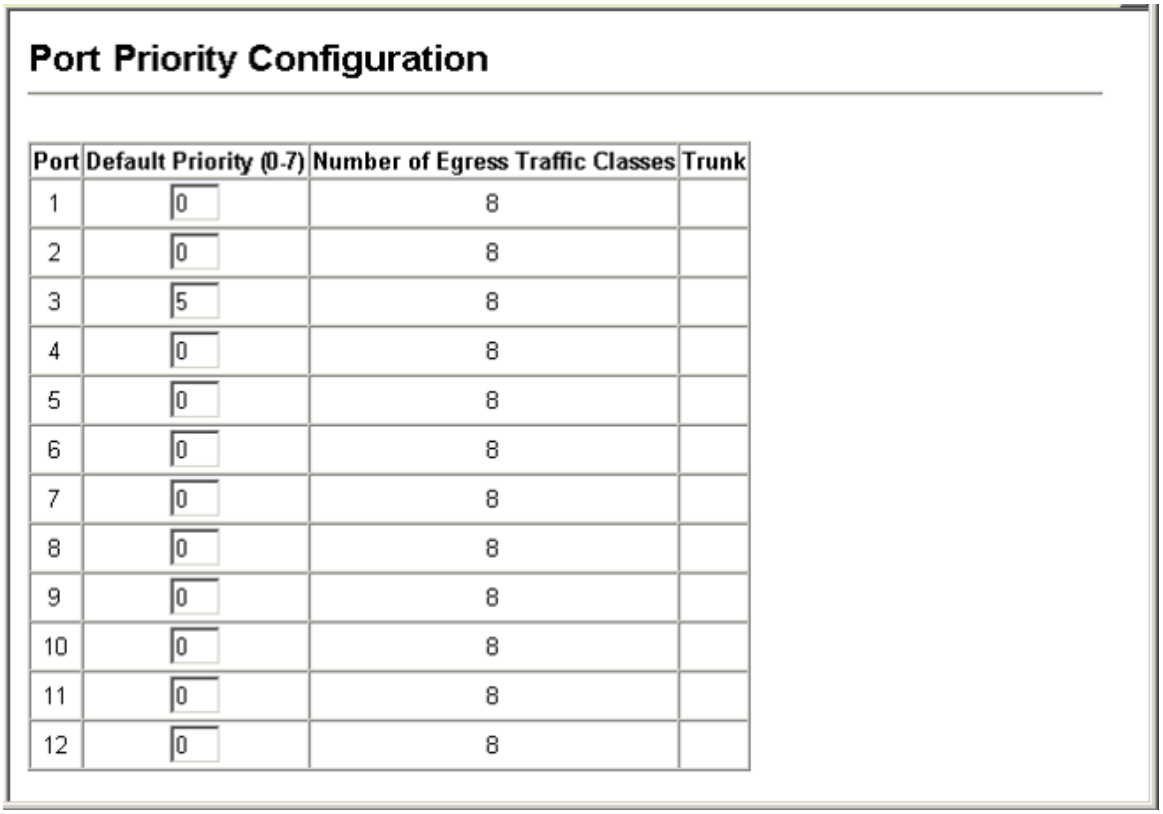
Command Attributes

- **Default Priority*** – The priority that is assigned to untagged frames received on the specified interface. (Range: 0 - 7, Default: 0)
- **Number of Egress Traffic Classes** – The number of queue buffers provided for each port.

Downloaded from www.Manualslib.com manuals search engine

* CLI displays this information as "Priority for untagged traffic."

Web – Click Priority, Default Port Priority or Default Trunk Priority. Modify the default priority for any interface, then click Apply.



Port Priority Configuration

Port	Default Priority (0-7)	Number of Egress Traffic Classes	Trunk
1	0	8	
2	0	8	
3	5	8	
4	0	8	
5	0	8	
6	0	8	
7	0	8	
8	0	8	
9	0	8	
10	0	8	
11	0	8	
12	0	8	

CLI – This example assigns a default priority of 5 to port 3.

```
Console(config)#interface ethernet 1/3 3-1
Console(config-if)#switchport priority default 5 3-78
Console(config-if)#end
Console#show interfaces switchport ethernet 1/5 3-14
Information of Eth 1/5
 Broadcast threshold: Enabled, 500 packets/second
 Lacp status: Disabled
 Ingress rate limit: disable,1000M bits per second
 Egress rate limit: disable,1000M bits per second
 VLAN membership mode: Hybrid
 Ingress rule: Disabled
 Acceptable frame type: All frames
 Native VLAN: 1
 Priority for untagged traffic: 5
 Gvrp status: Disabled
 Allowed Vlan:    1(u),
 Forbidden Vlan:
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Mapping CoS Values to Egress Queues

This switch processes Class of Service (CoS) priority tagged traffic by using eight priority queues for each port, with service schedules based on strict or Weighted Round Robin (WRR). Up to eight separate traffic priorities are defined in IEEE 802.1p. The default priority levels are assigned according to recommendations in the IEEE 802.1p standard as shown in the following table.

Queue	0	1	2	3	4	5	6	7
Priority	2	0	1	3	4	5	6	7

The priority levels recommended in the IEEE 802.1p standard for various network applications are shown in the following table. However, you can map the priority levels to the switch's output queues in any way that benefits application traffic for your own network.

Priority Level	Traffic Type
1	Background
2	(Spare)
0 (default)	Best Effort
3	Excellent Effort
4	Controlled Load
5	Video, less than 100 milliseconds latency and jitter
6	Voice, less than 10 milliseconds latency and jitter
7	Network Control

Command Attributes

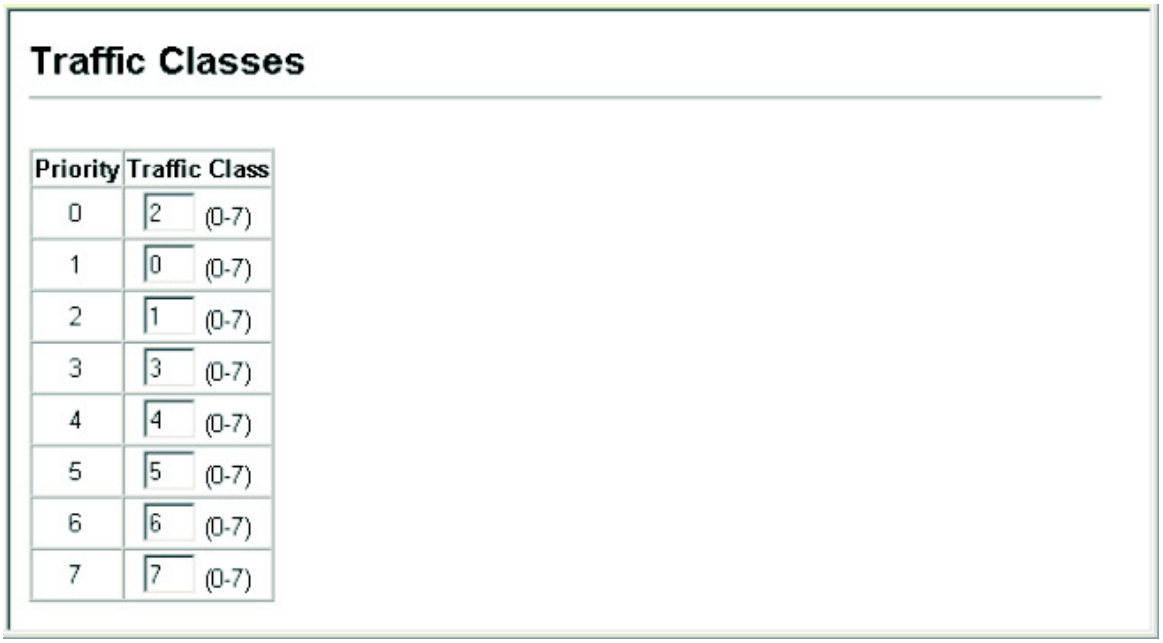
- **Priority** – CoS value. (Range: 0-7, where 7 is the highest priority)
- **Traffic Class*** – Output queue buffer. (Range: 0-7, where 7 is the highest CoS priority queue)

* CLI shows Queue ID.

Web – Click Priority, Traffic Classes. Mark an interface and click Select to display the current mapping of CoS values to output queues. Assign

Downloaded from www.Manualslib.com manuals search engine

priorities to the traffic classes (i.e., output queues) for the selected interface, then click Apply.



CLI – The following example shows how to change the CoS assignments to a one-to-one mapping.

```
Console(config)#interface ethernet 1/13-1
Console(config)#queue cos-map 0 0 3-81
Console(config)#queue cos-map 1 1
Console(config)#queue cos-map 2 2
Console(config)#exit
Console#show queue cos-map ethernet 1/13-84
Information of Eth 1/1
 Traffic Class : 0 1 2 3 4 5 6 7
 Priority Queue: 0 1 2 3 4 5 6 7
Information of Eth 1/2
 Traffic Class : 0 1 2 3 4 5 6 7
 Priority Queue: 0 1 2 3 4 5 6 7
.
.
.
```

* Mapping specific values for CoS priorities is implemented as an interface configuration command, but any changes will apply to the all interfaces on the switch.

Downloaded from www.Manualslib.com manuals search engine

Selecting the Queue Mode

You can set the switch to service the queues based on a strict rule that requires all traffic in a higher priority queue to be processed before lower priority queues are serviced, or use Weighted Round-Robin (WRR) queuing that specifies a relative weight of each queue. WRR uses a predefined relative weight for each queue that determines the percentage of service time the switch services each queue before moving on to the next queue. This prevents the head-of-line blocking that can occur with strict priority queuing.

Command Attributes

- **WRR** - Weighted Round-Robin shares bandwidth at the egress ports by using scheduling weights 1, 2, 4, 6, 8, 10, 12, 14 for queues 0 through 7 respectively. (This is the default selection.)

- **Strict** - Services the egress queues in sequential order, transmitting all traffic in the higher priority queues before servicing lower priority queues.

Web – Click Priority, Queue Mode. Select Strict or WRR, then click Apply.

CLI – The following sets the queue mode to strict priority service mode.

```
Console(config)#queue mode strict 3-83
Console(config)#exit
Console#show queue mode3-83

Queue mode: strict
Console#
```

Setting the Service Weight for Traffic Classes

This switch uses the Weighted Round Robin (WRR) algorithm to determine the frequency at which it services each priority queue. As

Downloaded from www.Manualslib.com manuals search engine

described in "Mapping CoS Values to Egress Queues" on page 3-174, the traffic classes are mapped to one of the eight egress queues provided for each port. You can assign a weight to each of these queues (and thereby to the corresponding traffic priorities). This weight sets the frequency at which each queue will be polled for service, and subsequently affects the response time for software applications assigned a specific priority value.

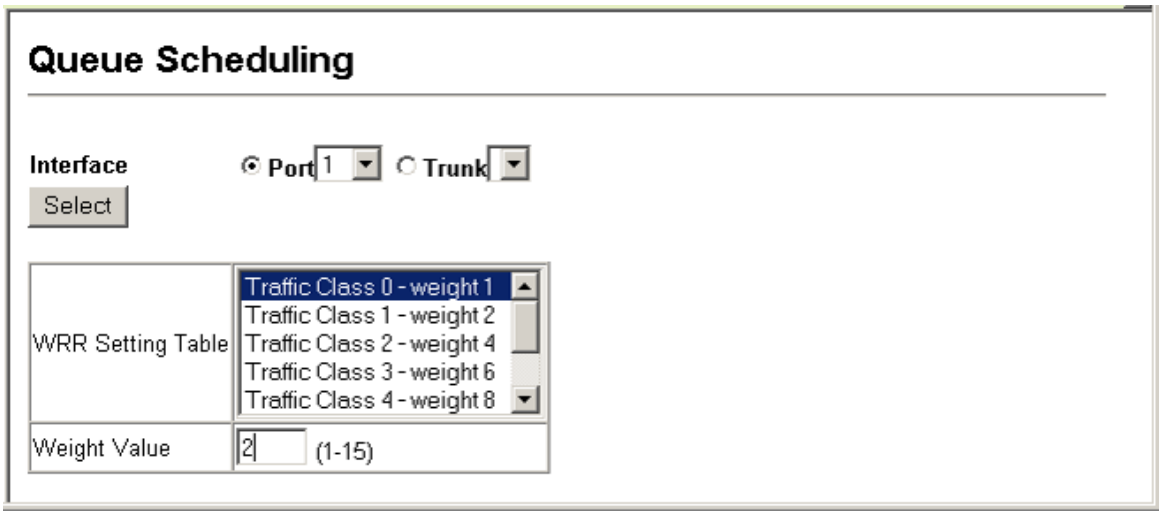
Command Attributes

- **WRR Setting Table*** – Displays a list of weights for each traffic class (i.e., queue).

- **Weight Value** – Set a new weight for the selected traffic class. (Range: 1-15)

* CLI shows Queue ID.

Web – Click Priority, Queue Scheduling. Select the interface, highlight a traffic class (i.e., output queue), enter a weight, then click Apply.



Downloaded from www.Manualslib.com manuals search engine

CLI – The following example shows how to assign WRR weights to each of the priority queues.

```
Console(config)#queue bandwidth 1 3 5 7 9 11 13 153-81
Console(config)#exit
Console#show queue bandwidth3-84
Information of Eth 1/1
 Queue ID  Weight
 --------  ------
    0        1
    1        3
    2        5
    3        7
    4        9
    5        11
    6        13
    7        15
Information of Eth 1/2
 Queue ID  Weight
.
.
.
```


Downloaded from www.Manualslib.com manuals search engine

Mapping Layer 3/4 Priorities to CoS Values

This switch supports several common methods of prioritizing layer 3/4 traffic to meet application requirements. Traffic priorities can be specified in the IP header of a frame, using the priority bits in the Type of Service (ToS) octet or the number of the TCP port. If priority bits are used, the ToS octet may contain three bits for IP Precedence or six bits for Differentiated Services Code Point (DSCP) service. When these services are enabled, the priorities are mapped to a Class of Service value by the switch, and the traffic then sent to the corresponding output queue.

Because different priority information may be contained in the traffic, this switch maps priority values to the output queues in the following manner:

- The precedence for priority mapping is IP Port Priority, IP Precedence or DSCP Priority, and then Default Port Priority.
- IP Precedence and DSCP Priority cannot both be enabled. Enabling one of these priority types will automatically disable the other.

Selecting IP Precedence/DSCP Priority

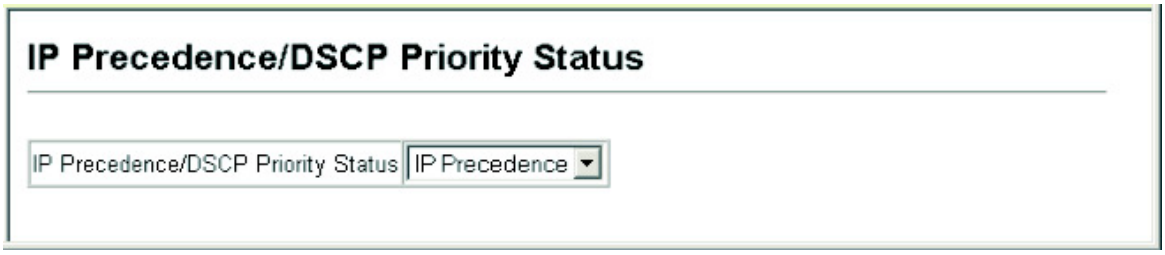
The switch allows you to choose between using IP Precedence or DSCP priority. Select one of the methods or disable this feature.

Command Attributes

- **Disabled** – Disables both priority services. (This is the default setting.)
- **IP Precedence** – Maps layer 3/4 priorities using IP Precedence.
- **IP DSCP** – Maps layer 3/4 priorities using Differentiated Services Code Point Mapping.

Web – Click Priority, IP Precedence/DSCP Priority Status. Select Disabled, IP Precedence or IP DSCP from the scroll-down menu.

Downloaded from www.Manualslib.com manuals search engine



CLI – The following example enables IP Precedence service on the switch.

```
Console(config)#map ip precedence3-88
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

Mapping IP Precedence

The Type of Service (ToS) octet in the IPv4 header includes three precedence bits defining eight different priority levels ranging from highest priority for network control packets to lowest priority for routine traffic. The default IP Precedence values are mapped one-to-one to Class of Service values (i.e., Precedence value 0 maps to CoS value 0, and so forth). Bits 6 and 7 are used for network control, and the other bits for various application types. ToS bits are defined in the following table.

Priority Level	Traffic Type	Priority Level	Traffic Type
7	Network Control	3	Flash
6	Internetwork Control	2	Immediate
5	Critical	1	Priority
4	Flash Override	0	Routine

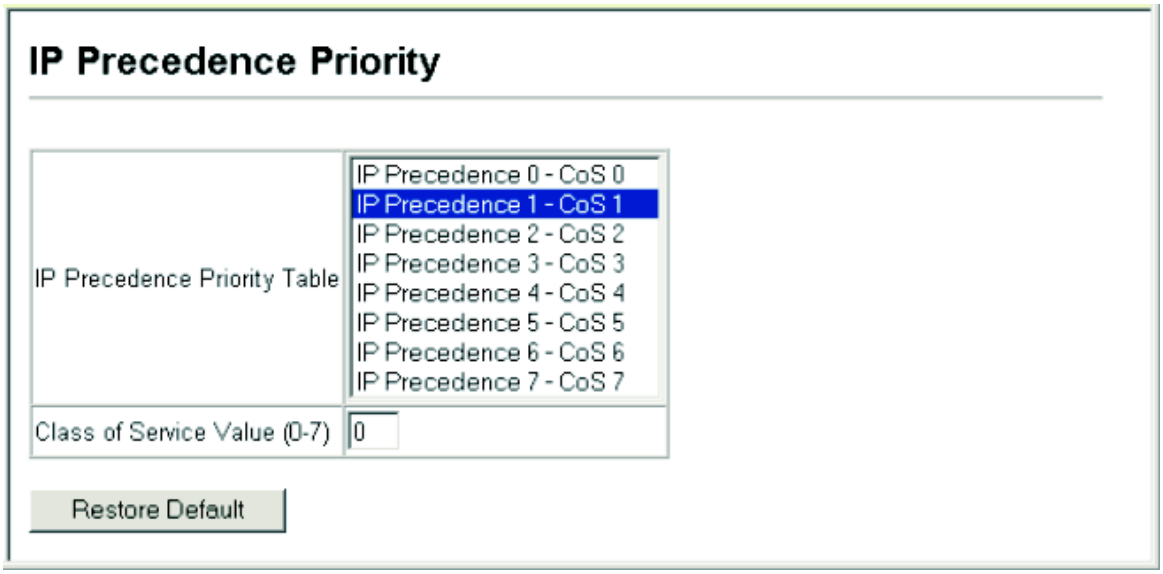
Command Attributes

- **IP Precedence Priority Table** – Shows the IP Precedence to CoS map.

- **Class of Service Value** – Maps a CoS value to the selected IP Precedence value. Note that "0" represents low priority and "7" represent high priority.

Downloaded from www.Manualslib.com manuals search engine

Web – Click Priority, IP Precedence Priority. Select an entry from the IP Precedence Priority Table, enter a value in the Class of Service Value field, and then click Apply.


IP Precedence Priority
IP Precedence Priority Table
IP Precedence 0 - CoS 0
IP Precedence 1 - CoS 1
IP Precedence 2 - CoS 2
IP Precedence 3 - CoS 3
IP Precedence 4 - CoS 4
IP Precedence 5 - CoS 5
IP Precedence 6 - CoS 6
IP Precedence 7 - CoS 7
Class of Service Value (0-7)
0
Restore Default

CLI – The following example globally enables IP Precedence service on the switch, maps IP Precedence value 1 to CoS value 0 (on port 1), and then displays the IP Precedence settings.

```
Console(config)#map ip precedence3-88
Console(config)#interface ethernet 1/13-1
Console(config-if)#map ip precedence 1 cos 03-88
Console(config-if)#end
Console#show map ip precedence ethernet 1/13-92
Precedence mapping status: disabled

 Port       Precedence COS
 ---------  ---------- ---
  Eth 1/ 1           0   0
  Eth 1/ 1           1   0
  Eth 1/ 1           2   2
  Eth 1/ 1           3   3
  Eth 1/ 1           4   4
  Eth 1/ 1           5   5
  Eth 1/ 1           6   6
  Eth 1/ 1           7   7
Console#
```

* Mapping specific values for IP Precedence is implemented as an interface configuration command, but any changes will apply to the all interfaces on the switch.

Downloaded from www.Manualslib.com manuals search engine

Mapping DSCP Priority

The DSCP is six bits wide, allowing coding for up to 64 different forwarding behaviors. The DSCP replaces the ToS bits, but it retains backward compatibility with the three precedence bits so that non-DSCP compliant, ToS-enabled devices, will not conflict with the DSCP mapping. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding. The DSCP default values are defined in the following table. Note that all the DSCP values that are not specified are mapped to CoS value 0.

IP DSCP Value	CoS Value
0	0
8	1
10, 12, 14, 16	2
18, 20, 22, 24	3
26, 28, 30, 32, 34, 36	4
38, 40, 42	5
48	6
46, 56	7

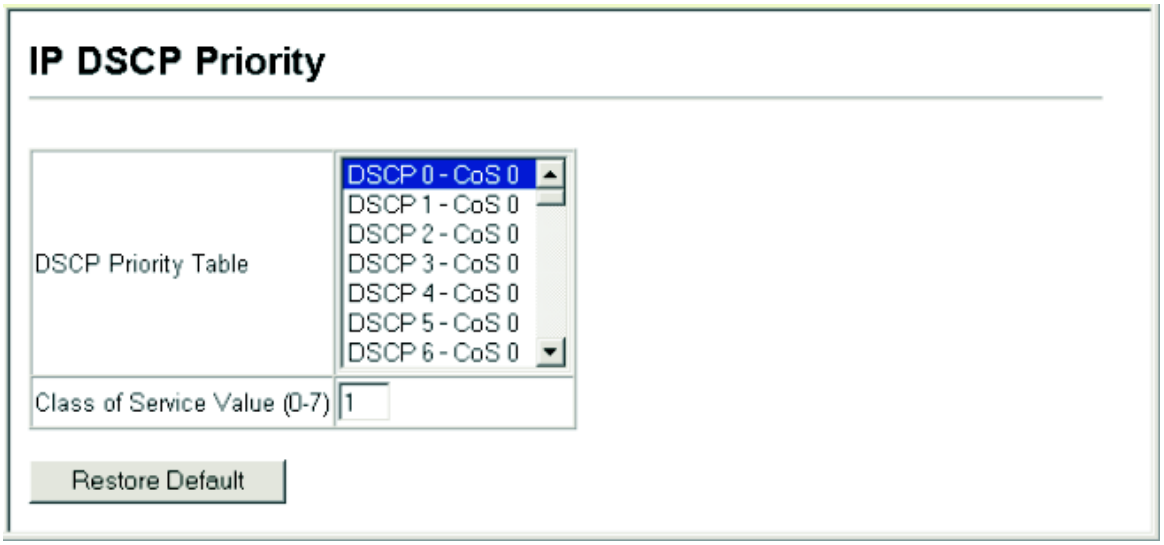
Command Attributes

- **DSCP Priority Table –** Shows the DSCP Priority to CoS map.
- **Class of Service Value –** Maps a CoS value to the selected DSCP Priority value. Note that "0" represents low priority and "7" represent high priority.

Note: IP DSCP settings apply to all interfaces.

Web – Click Priority, IP DSCP Priority. Select an entry from the DSCP table, enter a value in the Class of Service Value field, then click Apply.

Downloaded from www.Manualslib.com manuals search engine


IP DSCP Priority
DSCP Priority Table
DSCP 0 - CoS 0
DSCP 1 - CoS 0
DSCP 2 - CoS 0
DSCP 3 - CoS 0
DSCP 4 - CoS 0
DSCP 5 - CoS 0
DSCP 6 - CoS 0
Class of Service Value (0-7)
1
Restore Default

CLI – The following example globally enables DSCP Priority service on the switch, maps DSCP value 0 to CoS value 1 (on port 1), and then displays the DSCP Priority settings.

```
Console(config)#map ip dscp3-89
Console(config)#interface ethernet 1/13-1
Console(config-if)#map ip dscp 1 cos 03-90
Console(config-if)#end
Console#show map ip dscp ethernet 1/13-93
DSCP mapping status: disabled

 Port       DSCP COS
 ---------  ---- ---
  Eth 1/ 1     0   0
  Eth 1/ 1     1   0
  Eth 1/ 1     2   0
  Eth 1/ 1     3   0
.
.
.
  Eth 1/ 1    61   0
  Eth 1/ 1    62   0
  Eth 1/ 1    63   0
Console#
```

* Mapping specific values for IP DSCP is implemented as an interface configuration command, but any changes will apply to the all interfaces on the switch.

Downloaded from www.Manualslib.com manuals search engine

Mapping IP Port Priority

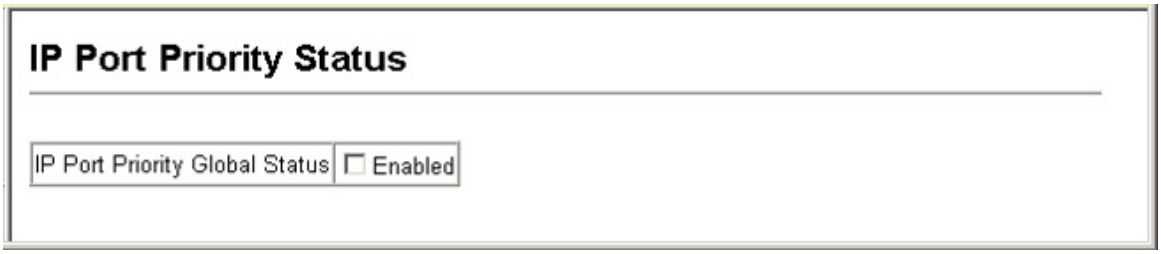
You can also map network applications to Class of Service values based on the IP port number (i.e., TCP/UDP port number) in the frame header. Some of the more common TCP service ports include: HTTP: 80, FTP: 21, Telnet: 23 and POP3: 110.

Command Attributes

- **IP Port Priority Status** – Enables or disables the IP port priority.
- **Interface** – Selects the port or trunk interface to which the settings apply.
- **IP Port Priority Table** – Shows the IP port to CoS map.
- **IP Port Number (TCP/UDP)** – Set a new IP port number.
- **Class of Service Value** – Sets a CoS value for a new IP port. Note that "0" represents low priority and "7" represent high priority.

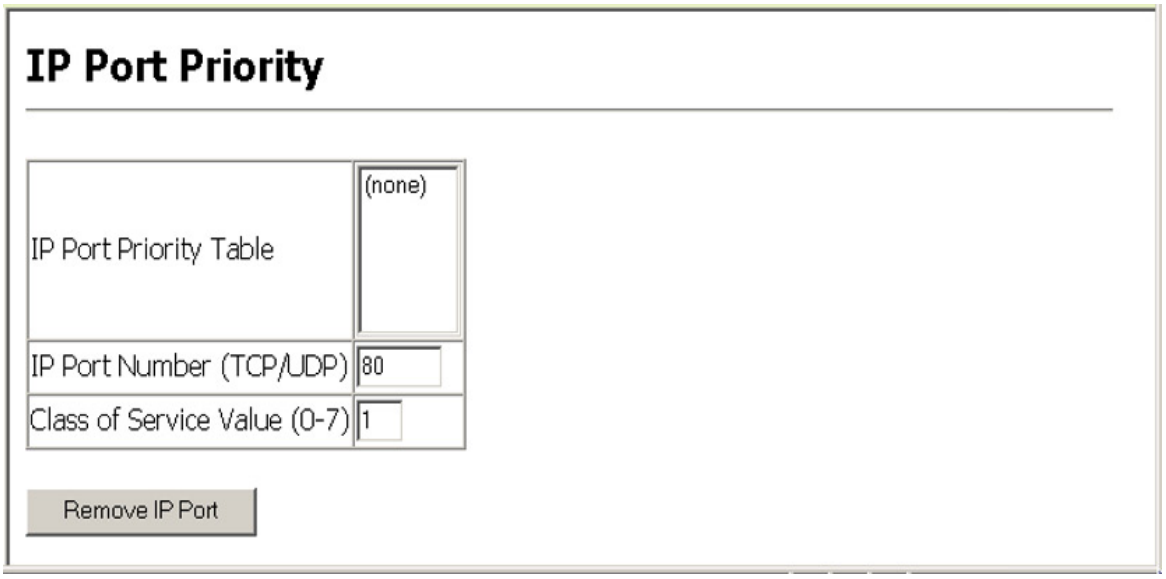
Note: IP Port Priority settings apply to all interfaces.

Web – Click Priority, IP Port Status. Set IP Port Priority Status to Enabled.



Click Priority, IP Port Priority. Select a port or trunk from the Interface field. Enter the port number for a network application in the IP Port Number box and the new CoS value in the Class of Service box, and then click Add IP Port.

Downloaded from www.Manualslib.com manuals search engine



* Mapping specific values for IP Port Priority is implemented as an interface configuration command, but any changes will apply to the all interfaces on the switch.

CLI – The following example globally enables IP Port Priority service on the switch, maps HTTP traffic (on port 1) to CoS value 0, and then displays the IP Port Priority settings.

```
Console(config)#map ip port3-85
Console(config)#interface ethernet 1/13-1
Console(config-if)#map ip port 80 cos 03-87
Console(config-if)#end
Console#show map ip port ethernet 1/53-91
TCP port mapping status: disabled

 Port      Port no. COS
 --------- -------- ---
  Eth 1/ 1       80   0
Console#
```

* Mapping specific values for IP Port Priority is implemented as an interface configuration command, but any changes will apply to the all interfaces on the switch.

Mapping CoS Values to ACLs

Use the ACL CoS Mapping page to set the output queue for packets matching an ACL rule as shown in the following table. Note that the specified CoS value is only used to map the matching packet to an output

Downloaded from www.Manualslib.com manuals search engine

queue; it is not written to the packet itself. For information on mapping the CoS values to output queues, see page 3-174.

Priority	0	1	2	3	4	5	6	7
Queue	1	2	0	3	4	5	6	7

Command Usage

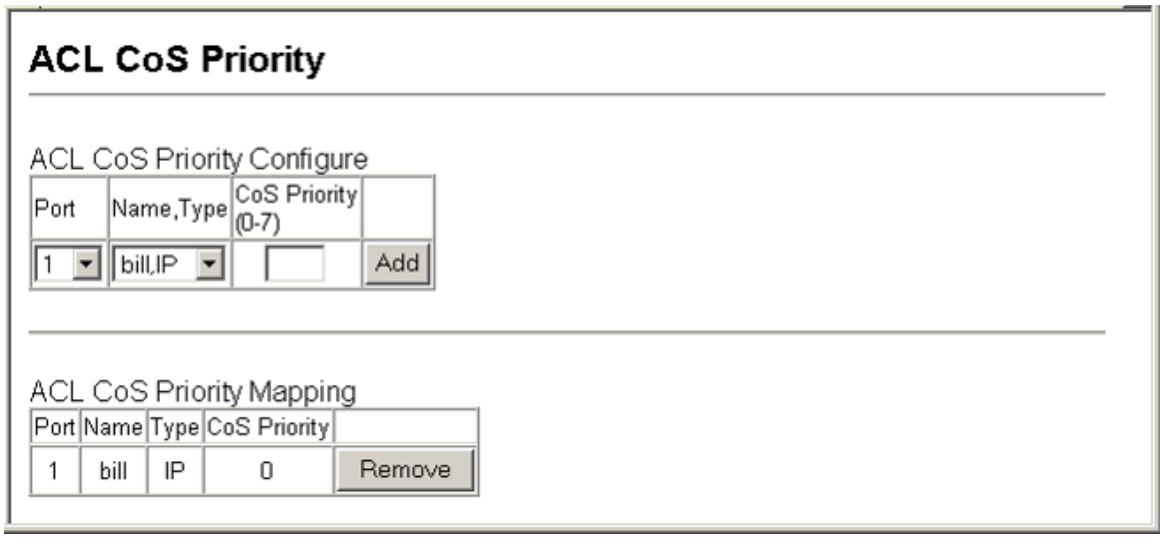
You must configure an ACL mask before you can map CoS values to the rule.

Command Attributes

- **Port** – Port identifier.
- **Name*** – Name of ACL.
- **Type** – Type of ACL (IP or MAC).
- **CoS Priority** – CoS value used for packets matching an IP ACL rule. (Range: 0-7)

* For information on configuring ACLs, see page 3-72.

Web – Click Priority, ACL CoS Priority. Select a port, select an ACL rule, specify a CoS priority, then click Add.



Downloaded from www.Manualslib.com manuals search engine

CLI – This example assigns a CoS value of zero to packets matching rules within the specified ACL on port 1.

```
Console(config)#interface ethernet 1/13-1
Console(config-if)#map access-list ip bill cos 03-128
Console(config-if)#
```

Changing Priorities Based on ACL Rules

You can change traffic priorities for frames matching the defined ACL rule. (This feature is commonly referred to as ACL packet marking.) This switch can change the IEEE 802.1p priority, IP Precedence, or DSCP Priority of IP frames; or change the IEEE 802.1p priority of Layer 2 frames. (This feature is commonly referred to as ACL packet marking.) Use the no form to remove the ACL marker.

Command Usage

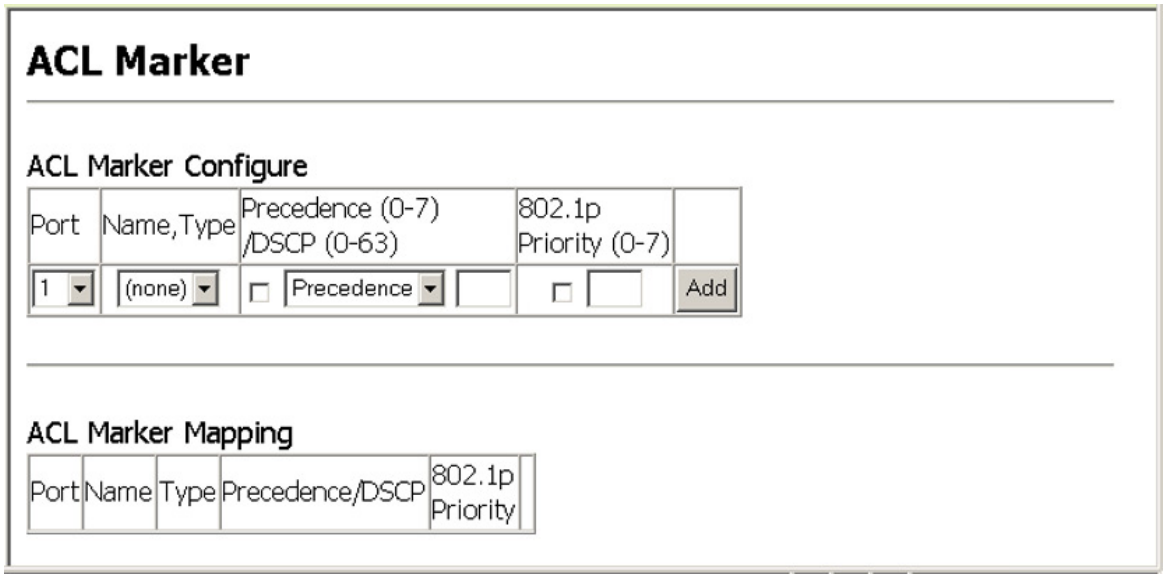
- You must configure an ACL mask before you can change priorities based on a rule.
- Traffic priorities may be included in the IEEE 802.1p priority tag. This tag is also incorporated as part of the overall IEEE 802.1Q VLAN tag. The 802.1p priority may be set for either Layer 2 or IP frames.
- The IP frame header also includes priority bits in the Type of Service (ToS) octet. The Type of Service octet may contain three bits for IP Precedence or six bits for Differentiated Services Code Point (DSCP) service. Note that the IP frame header can include either the IP Precedence or DSCP priority type.
- The precedence for priority mapping by this switch is IP Precedence or DSCP Priority, and then 802.1p priority.

Downloaded from www.Manualslib.com manuals search engine

Command Attributes

- **Port** – Port identifier.
- **Name*** – Name of ACL.
- **Type** – Type of ACL (IP or MAC).
- **Precedence** – IP Precedence value. (Range: 0-7)
- **DSCP** – Differentiated Services Code Point value. (Range: 0-63)
- **802.1p Priority** – Class of Service value in the IEEE 802.1p priority tag. (Range: 0-7; 7 is the highest priority)

Web – Click Priority, ACL Marker. Select a port and an ACL rule. To specify a ToS priority, mark the Precedence/DSCP check box, select Precedence or DSCP from the scroll-down box, and enter a priority. To specify an 802.1p priority, mark the 802.1p Priority check box, and enter a priority. Then click Add.



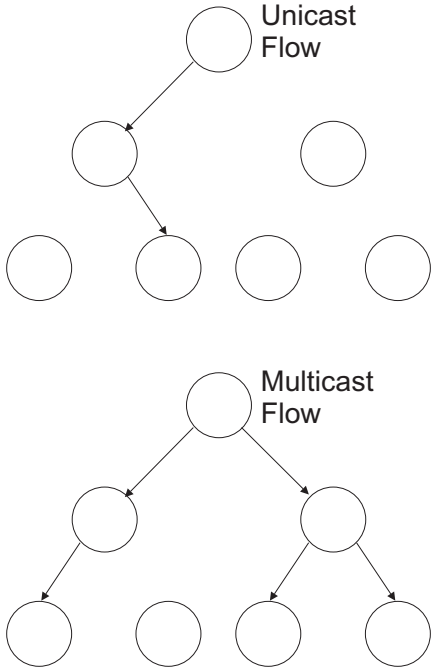
Downloaded from www.Manualslib.com manuals search engine

CLI – This example changes the DSCP priority for packets matching an IP ACL rule, and the 802.1p priority for packets matching a MAC ACL rule.

```
Console(config)#interface ethernet 1/13-1
Console(config-if)#match access-list ip bill set dscp 03-130
Console(config-if)#match access-list mac mike set priority 03-145
Console(config-if)#end
Console#show marking3-131
Interface ethernet 1/1
 match access-list IP bill set DSCP 0
 match access-list MAC a set priority 0
Console#
```

Multicast Filtering

Multicasting is used to support real-time applications such as videoconferencing or streaming audio. A multicast server does not have to establish a separate connection with each client. It merely broadcasts its service to the network, and any hosts that want to receive the multicast register with their local multicast switch/router. Although this approach reduces the network overhead required by a multicast server, the broadcast traffic must be carefully pruned at every multicast switch/router it passes through to ensure that traffic is only passed on to the hosts which subscribed to this service.



This switch uses IGMP (Internet Group Management Protocol) to query for any attached hosts that want to receive a specific multicast service. It identifies the ports containing hosts requesting to join the service and sends data out to those ports only. It then propagates the service request up to any neighboring multicast switch/router to ensure that it will

Downloaded from www.Manualslib.com manuals search engine

continue to receive the multicast service. This procedure is called multicast filtering.

The purpose of IP multicast filtering is to optimize a switched network's performance, so multicast packets will only be forwarded to those ports containing multicast group hosts or multicast routers/switches, instead of flooding traffic to all ports in the subnet (VLAN).

This switch not only supports IP multicast filtering by passively monitoring IGMP query and report messages and multicast routing probe messages to register end-stations as multicast group members, but also supports the DVMRP and PIM-DM multicast routing protocols required to forward multicast traffic to other subnets (page 3-323 and 3-334).

IGMP Protocol

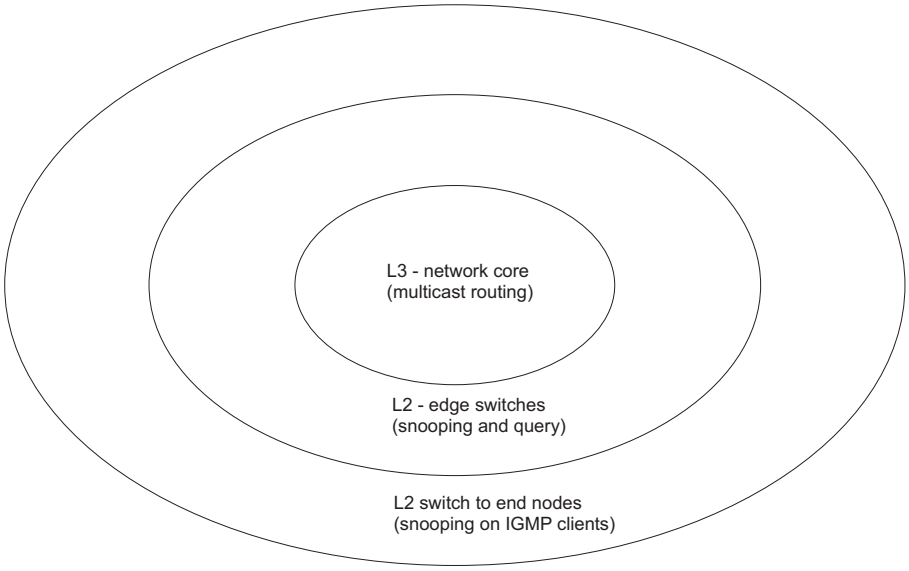
The Internet Group Management Protocol (IGMP) runs between hosts and their immediately adjacent multicast router/switch. IGMP is a multicast host registration protocol that allows any host to inform its local router that it wants to receive transmissions addressed to a specific multicast group.

A router, or multicast-enabled switch, can periodically ask their hosts if they want to receive multicast traffic. If there is more than one router/switch on the LAN performing IP multicasting, one of these devices is elected "querier" and assumes the role of querying the LAN for group members. It then propagates the service requests on to any adjacent multicast switch/router to ensure that it will continue to receive the multicast service.

Based on the group membership information learned from IGMP, a router/switch can determine which (if any) multicast traffic needs to be forwarded to each of its ports. At Layer 3, multicast routers use this information, along with a multicast routing protocol such as DVMRP or PIM, to support IP multicasting across the Internet.

Downloaded from www.Manualslib.com manuals search engine

Note that IGMP neither alters nor routes IP multicast packets. A multicast routing protocol must be used to deliver IP multicast packets across different subnetworks. Therefore, when DVMRP or PIM routing is enabled for a subnet on this switch, you also need to enable IGMP.



Layer 2 IGMP (Snooping and Query)

IGMP Snooping and Query – If multicast routing is not supported on other switches in your network, you can use IGMP Snooping and IGMP Query (page 3-193) to monitor IGMP service requests passing between multicast clients and servers, and dynamically configure the switch ports which need to forward multicast traffic.

Static IGMP Router Interface – If IGMP snooping cannot locate the IGMP querier, you can manually designate a known IGMP querier (i.e., a multicast router/switch) connected over the network to an interface on your switch (page 3-196). This interface will then join all the current multicast groups supported by the attached router/switch to ensure that multicast traffic is passed to all appropriate interfaces within the switch.

Static IGMP Host Interface – For multicast applications that you need to control more carefully, you can manually assign a multicast service to specific interfaces on the switch (page 3-199).

Downloaded from www.Manualslib.com manuals search engine

IGMP Query (Layer 2 or 3) – IGMP Query can only be enabled globally at Layer 2, but can be enabled for individual VLAN interfaces at Layer 3 (page 3-200). However, note that Layer 2 query is disabled if Layer 3 query is enabled.

Configuring IGMP Snooping and Query Parameters

You can configure the switch to forward multicast traffic intelligently. Based on the IGMP query and report messages, the switch forwards traffic only to the ports that request multicast traffic. This prevents the switch from broadcasting the traffic to all ports and possibly disrupting network performance.

Command Usage

- **IGMP Snooping** – This switch can passively snoop on IGMP Query and Report packets transferred between IP multicast routers/switches and IP multicast host groups to identify the IP multicast group members. It simply monitors the IGMP packets passing through it, picks out the group registration information, and configures the multicast filters accordingly.

- **IGMP Querier** – A router, or multicast-enabled switch, can periodically ask their hosts if they want to receive multicast traffic. If there is more than one router/switch on the LAN performing IP multicasting, one of these devices is elected "querier" and assumes the role of querying the LAN for group members. It then propagates the service requests on to any upstream multicast switch/router to ensure that it will continue to receive the multicast service.

Note: Multicast routers use this information, along with a multicast routing protocol such as DVMRP or PIM, to support IP multicasting across the Internet.

Command Attributes

- **IGMP Status** — When enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic. This

Downloaded from www.Manualslib.com manuals search engine

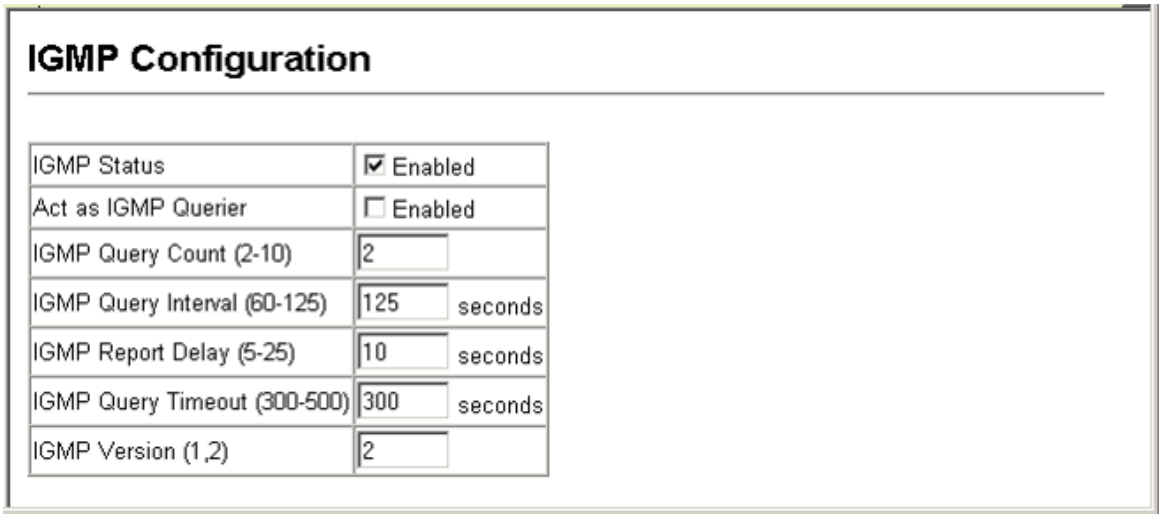
is also referred to as IGMP Snooping. (Default: Enabled)

- **Act as IGMP Querier** — When enabled, the switch can serve as the Querier, which is responsible for asking hosts if they want to receive multicast traffic. (Default: Disabled)
- **IGMP Query Count** — Sets the maximum number of queries issued for which there has been no response before the switch takes action to drop a client from the multicast group. (Range: 2-10, Default: 2)
- **IGMP Query Interval** — Sets the frequency at which the switch sends IGMP host-query messages. (Range: 60-125 seconds, Default: 125)
- **IGMP Report Delay** — Sets the time between receiving an IGMP Report for an IP multicast address on a port before the switch sends an IGMP Query out of that port and removes the entry from its list. (Range: 5-30 seconds, Default: 10)
- **IGMP Query Timeout** — The time the switch waits after the previous querier stops before it considers the router port (i.e., the interface which had been receiving query packets) to have expired. (Range: 300-500 seconds, Default: 300)
- **IGMP Version** — Sets the protocol version for compatibility with other devices on the network. (Range: 1-2; Default: 2)

Notes: **1.** All systems on the subnet must support the same version.
2. Some attributes are only enabled for IGMPv2, including IGMP Report Delay and IGMP Query Timeout.

Web – Click IGMP Snooping, IGMP Configuration. Adjust the IGMP settings as required, and then click Apply. (The default settings are shown below.)

Downloaded from www.Manualslib.com manuals search engine



CLI – This example modifies the settings for multicast filtering, and then displays the current status.

```
Console(config)#ip igmp snooping3-96
Console(config)#ip igmp snooping querier3-100
Console(config)#ip igmp snooping query-count 103-101
Console(config)#ip igmp snooping query-interval 1003-102
Console(config)#ip igmp snooping query-max-response-time 203-102
Console(config)#ip igmp snooping query-time-out 3003-104
Console(config)#ip igmp snooping version 23-97
Console(config)#exit
Console#show ip igmp snooping3-98
 Service status          : Enabled
 Querier status          : Enabled
 Query count             : 10
 Query interval          : 100 sec
 Query max response time : 20 sec
 Router port expire time: 300 sec
 IGMP snooping version   : Version 2
Console#
```

Displaying Interfaces Attached to a Multicast Router

Multicast routers that are attached to ports on the switch use information obtained from IGMP, along with a multicast routing protocol such as DVMRP or PIM, to support IP multicasting across the Internet. These routers may be dynamically discovered by the switch or statically assigned to an interface on the switch.

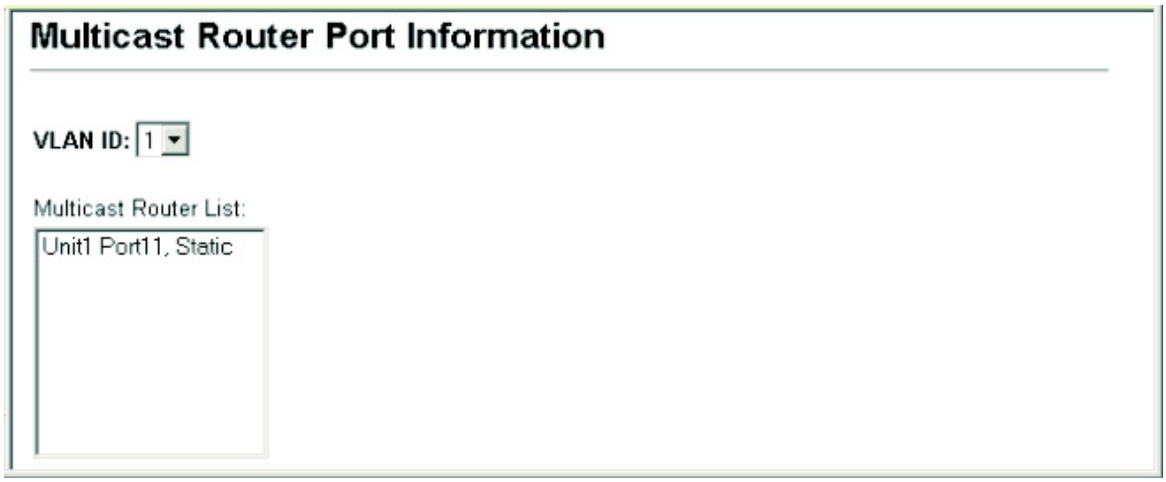
Downloaded from www.Manualslib.com manuals search engine

You can use the Multicast Router Port Information page to display the ports on this switch attached to a neighboring multicast router/switch for each VLAN ID.

Command Attributes

- **VLAN ID** – ID of configured VLAN (1-4094).
- **Multicast Router List** – Multicast routers dynamically discovered by this switch or those that are statically assigned to an interface on this switch.

Web – Click IGMP Snooping, Multicast Router Port Information. Select the required VLAN ID from the scroll-down list to display the associated multicast routers.



CLI – This example shows that Port 11 has been statically configured as a port attached to a multicast router.

```
Console#show ip igmp snooping mrouter vlan 13-106
 VLAN M'cast Router Port Type
 ---- ------------------ -------
    1           Eth 1/11 Static
```

Specifying Static Interfaces for a Multicast Router

Depending on your network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router/ switch connected over the network to an

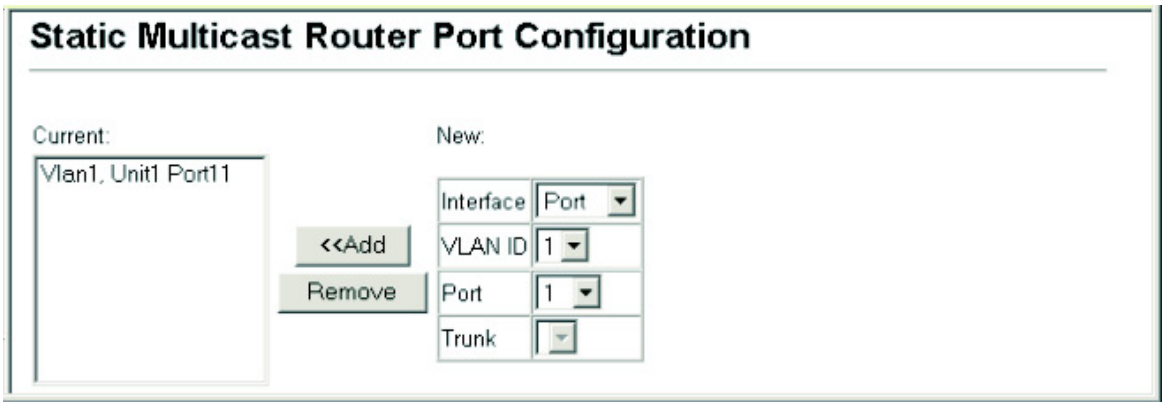
Downloaded from www.Manualslib.com manuals search engine

interface (port or trunk) on your switch, you can manually configure the interface (and a specified VLAN) to join all the current multicast groups supported by the attached router. This can ensure that multicast traffic is passed to all the appropriate interfaces within the switch.

Command Attributes

- **Interface** – Activates the Port or Trunk scroll down list.
- **VLAN ID** – Selects the VLAN to propagate all multicast traffic coming from the attached multicast router.
- **Port** or **Trunk** – Specifies the interface attached to a multicast router.

Web – Click IGMP Snooping, Static Multicast Router Port Configuration. Specify the interfaces attached to a multicast router, indicate the VLAN which will forward all the corresponding multicast traffic, and then click Add. After you have finished adding interfaces to the list, click Apply.



CLI – This example configures port 11 as a multicast router port within VLAN 1.

```
Console(config)#ip igmp snooping vlan 1 mrouter ethernet 1/113-105
Console(config)#exit
Console#show ip igmp snooping mrouter vlan 13-106
 VLAN M'cast Router Port Type
 ---- ----------------- -------
    1           Eth 1/11  Static
```


Downloaded from www.Manualslib.com manuals search engine

Displaying Port Members of Multicast Services

You can display the port members associated with a specified VLAN and multicast service.

Command Attribute

- **VLAN ID** – Selects the VLAN for which to display port members.
- **Multicast IP Address** – The IP address for a specific multicast service.
- **Multicast Group Port List** – Shows the interfaces that have already been assigned to the selected VLAN to propagate a specific multicast service.

Web – Click IGMP Snooping, IP Multicast Registration Table. Select a VLAN ID and the IP address for a multicast service from the scroll-down lists. The switch will display all the interfaces that are propagating this multicast service.

CLI – This example displays all the known multicast services supported on VLAN 1, along with the ports propagating the corresponding services.

Downloaded from www.Manualslib.com manuals search engine

The Type field shows if this entry was learned dynamically or was statically configured.

```
Console#show bridge 1 multicast vlan 13-99
 VLAN M'cast IP addr. Member ports Type
 ---- --------------- ------------ -------
    1      224.1.1.12      Eth1/12    USER
    1       224.1.2.3      Eth1/12    IGMP
Console#
```

Assigning Ports to Multicast Services

Multicast filtering can be dynamically configured using IGMP Snooping and IGMP Query messages as described in "Configuring IGMP Snooping and Query Parameters" on page 3-193. For certain applications that require tighter control, you may need to statically configure a multicast service on the switch. First add all the ports attached to participating hosts to a common VLAN, and then assign the multicast service to that VLAN group.

Command Usage

- Static multicast addresses are never aged out.
- When a multicast address is assigned to an interface in a specific VLAN, the corresponding traffic can only be forwarded to ports within that VLAN.

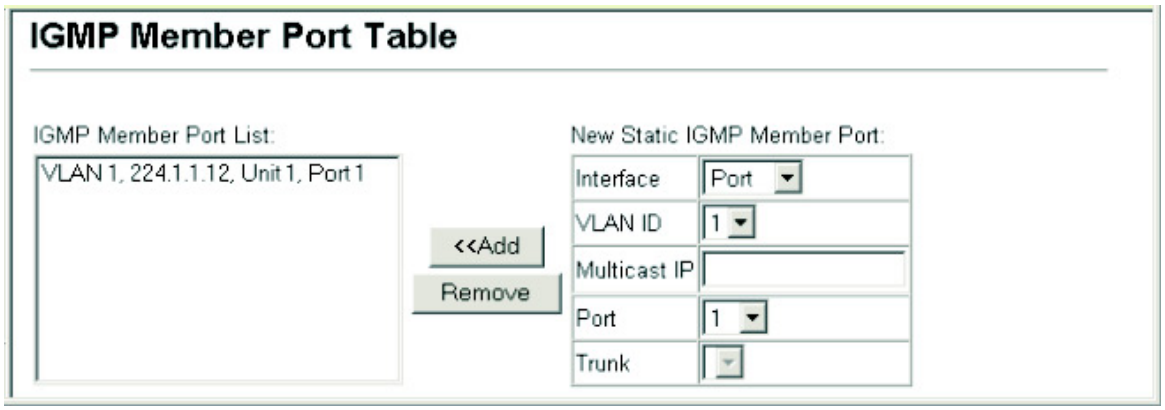
Command Attribute

- **Interface** – Activates the Port or Trunk scroll down list.
- **VLAN ID** – Selects the VLAN to propagate all multicast traffic coming from the attached multicast router/switch.
- **Multicast IP** – The IP address for a specific multicast service
- **Port** or **Trunk** – Specifies the interface attached to a multicast router/switch.

Web – Click IGMP Snooping, IGMP Member Port Table. Specify the interface attached to a multicast service (via an IGMP-enabled switch or

Downloaded from www.Manualslib.com manuals search engine

multicast router), indicate the VLAN that will propagate the multicast service, specify the multicast IP address, and click Add. After you have completed adding ports to the member list, click Apply.



CLI – This example assigns a multicast address to VLAN 1, and then displays all the known multicast services supported on VLAN 1.

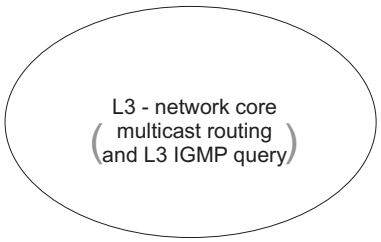
```
Console(config)#ip igmp snooping vlan 1 static 224.1.1.12
ethernet 1/123-96
Console(config)#exit
Console#show mac-address-table multicast vlan 13-99
 VLAN M'cast IP addr. Member ports Type
 ---- --------------- ------------ -------
    1      224.1.1.12      Eth1/12    USER
    1       224.1.2.3      Eth1/12    IGMP
Console#
```

Layer 3 IGMP (Query used with Multicast Routing)

IGMP Snooping – IGMP Snooping is a Layer 2 function (page 3-193) that can be used to provide multicast filtering when no other switches in the network support multicast routing. (Note that IGMP Snooping can only be globally enabled.)

IGMP Query – Multicast query is used to poll each known multicast group for active members, and dynamically configure the switch ports which need to forward multicast traffic. Although the implementation differs slightly, IGMP Query is used in conjunction with both Layer 2 IGMP Snooping and multicast routing. Note that when using IGMP Snooping, multicast query is automatically enabled. (See "Configuring IGMP Snooping and Query Parameters" on page 3-193.)

Downloaded from www.Manualslib.com manuals search engine



Layer 3 IGMP – This protocol includes a form of multicast query specifically designed to work with multicast routing. A router periodically asks its hosts if they want to receive multicast traffic. It then propagates service requests on to any upstream multicast router to ensure that it will continue to receive the multicast service. Layer 3 IGMP can be enabled for individual VLAN interfaces (page 3-200). (Note that Layer 2 snooping and query is disabled if Layer 3 IGMP is enabled.)

Configuring IGMP Interface Parameters

This switch uses IGMP (Internet Group Management Protocol) to query for any attached hosts that want to receive a specific multicast service. The hosts may respond with several types of IP multicast messages. Hosts respond to queries with report messages that indicate which groups they want to join or the groups to which they already belong. If a router does not receive a report message within a specified period of time, it will prune that interface from the multicast tree. A host can also submit a join message at any time without waiting for a query from the router. Host can also signal when they no longer want to receive traffic for a specific group by sending a leave-group message.

These IGMP messages are used by the router to identify ports containing multicast hosts and to restrict the downstream flow of multicast data to only these ports. If more than one router on the LAN is performing IP multicasting, one of these is elected as the "querier" and assumes the role of querying for group members. It then propagates the service request up to any neighboring multicast router to ensure that it will continue to receive the multicast service. The following parameters are used to control Layer 3 IGMP and query functions.

Command Attributes

- **VLAN** (Interface) – VLAN interface bound to a primary IP address.

Downloaded from www.Manualslib.com manuals search engine

(Range: 1-4094)

- **IGMP Protocol Status** (Admin Status) – Enables IGMP on a VLAN interface. (Default: Disabled)

- **Last Member Query Interval** – A multicast client sends an IGMP leave message when it leaves a group. The router then checks to see if this was the last host in the group by sending an IGMP query and starting a timer based on this command. If no reports are received before the timer expires, the group is deleted. (Range: 0-25 seconds; Default: 1 second)

  - This value may be tuned to modify the leave latency of the network. A reduced value results in reduced time to detect the loss of the last member of a group.

- **Max Query Response Time** – Configures the maximum response time advertised in IGMP queries. (Range: 0-25 seconds; Default: 10 seconds)

  - The switch must be using IGMPv2 for this command to take effect.
  - This command defines how long any responder (i.e., client or router) still in the group has to respond to a query message before the router deletes the group.
  - By varying the Maximum Query Response Time, you can tune the burstiness of IGMP messages passed on the subnet; where larger values make the traffic less bursty, as host responses are spread out over a larger interval.
  - The number of seconds represented by the maximum response interval must be less than the Query Interval.

- **Query Interval** – Configures the frequency at which host query messages are sent. (Range: 1-255; Default: 125 seconds)

  - Multicast routers send host query messages to determine the interfaces that are connected to downstream hosts requesting a

Downloaded from www.Manualslib.com manuals search engine

specific multicast service. Only the designated multicast router for a subnet sends host query messages, which are addressed to the multicast address 224.0.0.1.

- For IGMP Version 1, the designated router is elected according to the multicast routing protocol that runs on the LAN. But for IGMP Version 2, the designated querier is the lowest IP-addressed multicast router on the subnet.

- **Robustness Variable** – Specifies the robustness (i.e., expected packet loss) for this interface. The robustness value is used in calculating the appropriate range for other IGMP variables, such as the Group Membership Interval (**Last Member Query Interval**), as well as the Other Querier Present Interval, and the Startup Query Count (RFC 2236). (Range: 1-255; Default: 2)

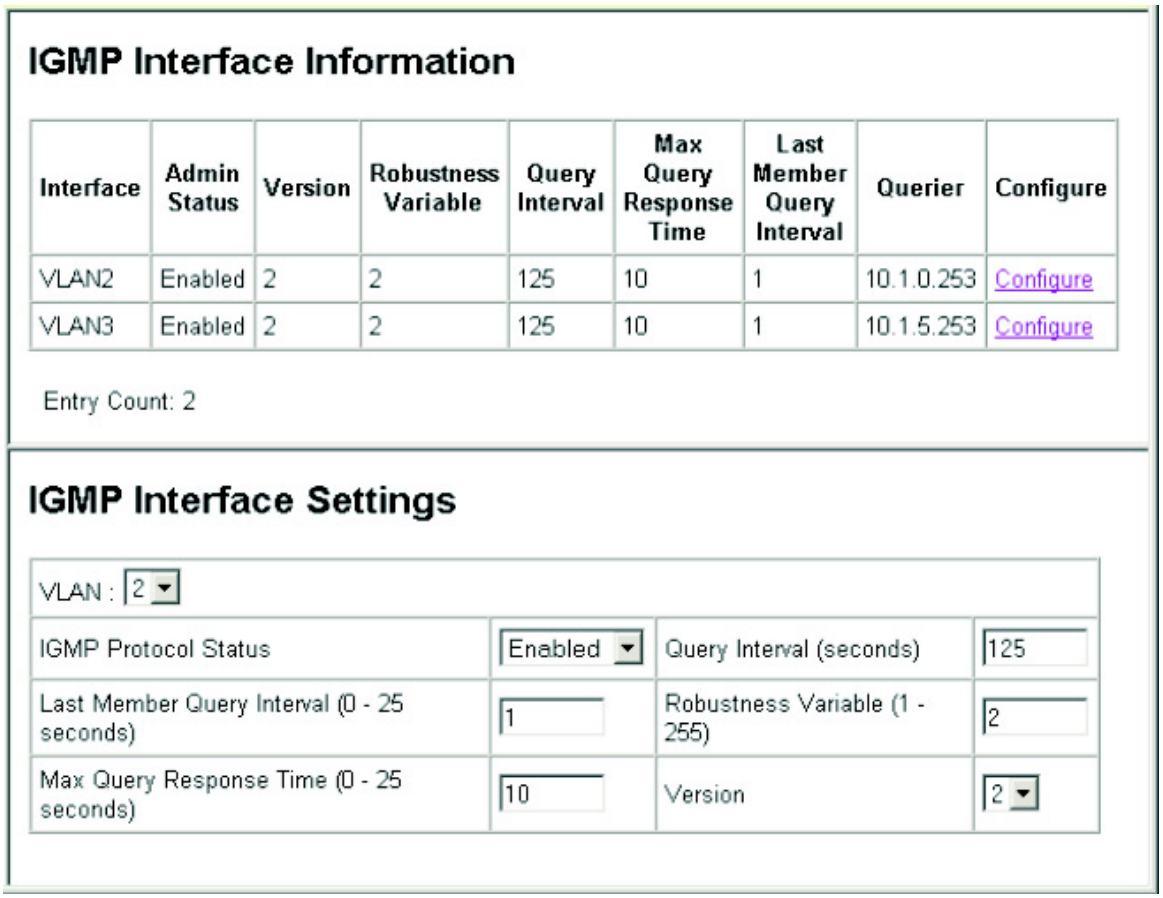
- **Version** – Configures the IGMP version used on an interface. (Options: Version 1 or 2; Default: Version 2)

  - All routers on the subnet must support the same version. However, the multicast hosts on the subnet may support either IGMP version 1 or 2.
  - The switch must be set to version 2 to enable the **Max Query Response Time**.

- **Querier** – Device currently serving as the IGMP querier for this multicast service.

Downloaded from www.Manualslib.com manuals search engine

Web – Click IP, IGMP, Interface Settings. Specify each interface that will support IGMP (Layer 3), specify the IGMP parameters for each interface, then click Apply.



IGMP Interface Information

Interface	Admin Status	Version	Robustness Variable	Query Interval	Max Query Response Time	Last Member Query Interval	Querier	Configure
VLAN2	Enabled	2	2	125	10	1	10.1.0.253	Configure
VLAN3	Enabled	2	2	125	10	1	10.1.5.253	Configure

Entry Count: 2

IGMP Interface Settings

VLAN : 2			
IGMP Protocol Status	Enabled	Query Interval (seconds)	125
Last Member Query Interval (0 - 25 seconds)	1	Robustness Variable (1 - 255)	2
Max Query Response Time (0 - 25 seconds)	10	Version	2

CLI – This example configures the IGMP parameters for VLAN 1.

```
Console(config)#interface vlan 13-57
Console(config-if)#ip igmp3-107
Console(config-if)#ip igmp last-memb-query-interval 103-111
Console(config-if)#ip igmp max-resp-interval 203-110
Console(config-if)#ip igmp query-interval 1003-110
Console(config-if)#ip igmp robustval 33-108
Console(config-if)#ip igmp version 13-112
Console(config-if)#end
Console#show ip igmp interface vlan 13-113
Vlan 1 is up
  IGMP is enable, version is 2
  Robustness variable is 2
  Query interval is 125 sec
  Query Max Response Time is 10 sec, Last Member Query Interval is 1 sec
  Querier is 10.1.0.253
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Displaying Multicast Group Information

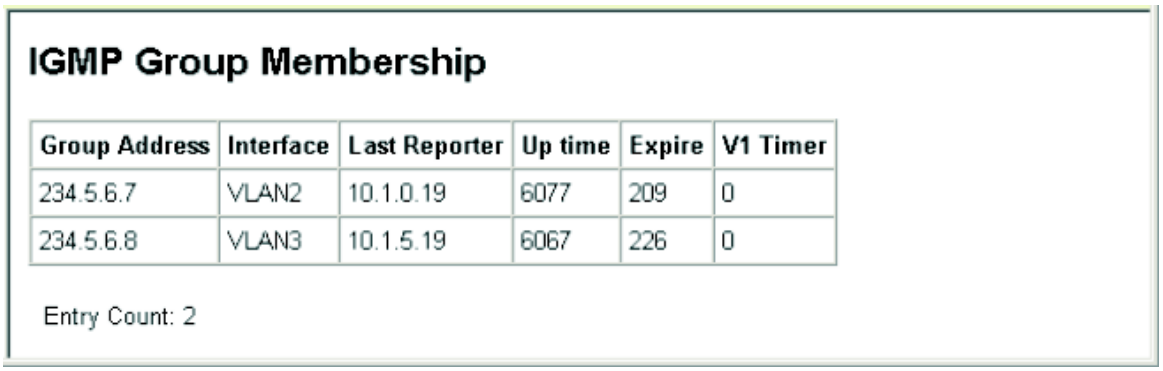
When IGMP (Layer 3) is enabled on this switch the current multicast groups learned via IGMP can be displayed in the IP/IGMP/Group Information page. When IGMP (Layer 3) is disabled and IGMP (Layer 2) is enabled, you can view the active multicast groups in the IGMP Snooping/IP Multicast Registration Table (see page 3-198).

Command Attributes

- **Group Address** – IP multicast group address with subscribers directly attached or downstream from this switch.
- **Interface** – The interface on this switch that has received traffic directed to the multicast group address.
- **Last Reporter** – The IP address of the source of the last membership report received for this multicast group address on this interface. If no membership report has been received, this object has the value 0.0.0.0.
- **Up time** – The time elapsed since this entry was created.
- **Expire** – The time remaining before this entry will be aged out. (Default: 260 seconds)
- **V1 Timer** – The time remaining until the switch assumes that there are no longer any IGMP Version 1 members on the IP subnet attached to this interface. (Default: 400 seconds)
    - If the switch receives an IGMP Version 1 Membership Report, it sets a timer to note that there are Version 1 hosts present which are members of the group for which it heard the report.
    - If there are Version 1 hosts present for a particular group, the switch will ignore any Leave Group messages that it receives for that group.

Web – Click IP, IGMP, IGMP Group Membership.

Downloaded from www.Manualslib.com manuals search engine



IGMP Group Membership

Group Address	Interface	Last Reporter	Up time	Expire	V1 Timer
234.5.6.7	VLAN2	10.1.0.19	6077	209	0
234.5.6.8	VLAN3	10.1.5.19	6067	226	0

Entry Count: 2

CLI – The following shows the IGMP groups currently active on VLAN 1.

```
Console#show ip igmp groups vlan 1-3-114

 GroupAddress    InterfaceVlan   Lastreporter    Uptime   Expire   V1Timer
--------------- --------------- --------------- -------- -------- ---------
      234.5.6.8               1       10.1.5.19     7068      220         0
Console#
```

Configuring Domain Name Service

The Domain Naming System (DNS) service on this switch allows host names to be mapped to IP addresses using static table entries or by redirection to other name servers on the network. When a client device designates this switch as a DNS server, the client will attempt to resolve host names into IP addresses by forwarding DNS queries to the switch, and waiting for a response.

You can manually configure entries in the DNS table used for mapping domain names to IP addresses, configure default domain names, or specify one or more name servers to use for domain name to address translation.

Configuring General DNS Server Parameters

Command Usage

- To enable DNS service on this switch, first configure one or more name servers, and then enable domain lookup status.

- To append domain names to incomplete host names received from a

Downloaded from www.Manualslib.com manuals search engine

DNS client (i.e., not formatted with dotted notation), you can specify a default domain name or a list of domain names to be tried in sequential order.

- If there is no domain list, the default domain name is used. If there is a domain list, the default domain name is not used.
- When an incomplete host name is received by the DNS server on this switch and a domain name list has been specified, the switch will work through the domain list, appending each domain name in the list to the host name, and checking with the specified name servers for a match.
- When more than one name server is specified, the servers are queried in the specified sequence until a response is received, or the end of the list is reached with no response.
- Note that if all name servers are deleted, DNS will automatically be disabled.

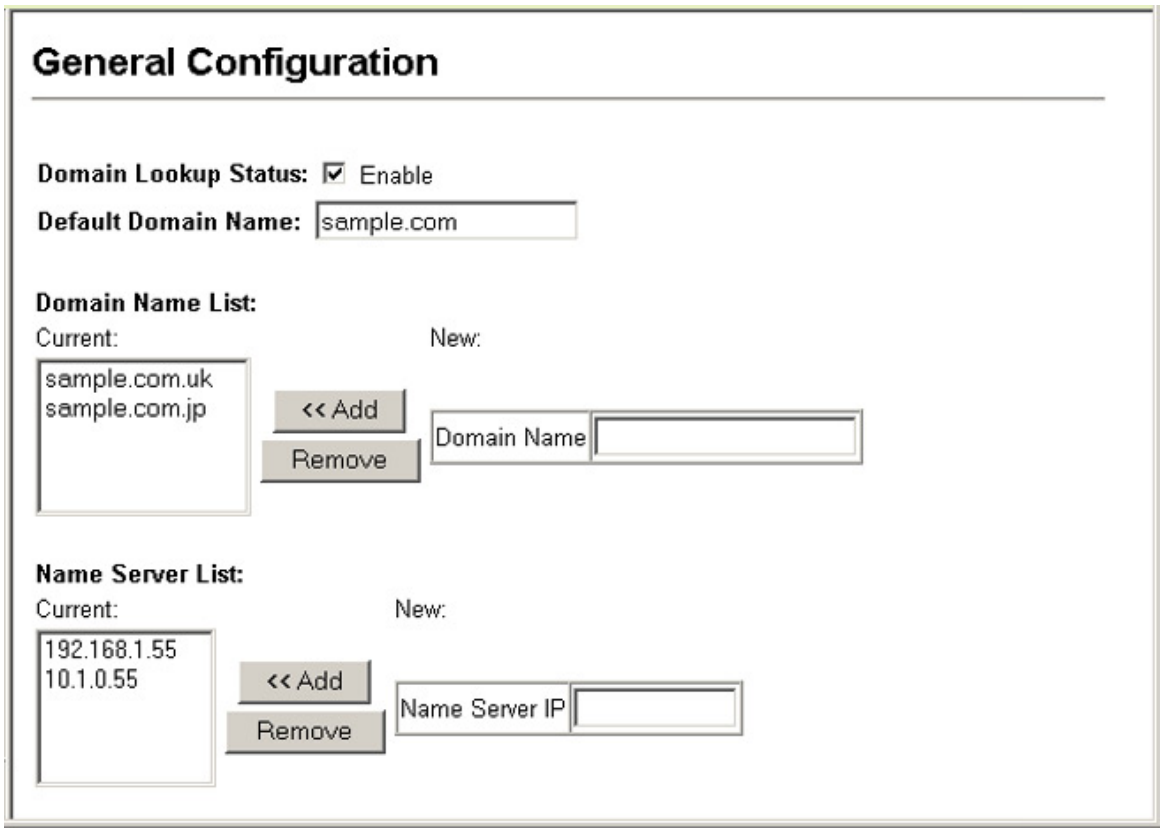
Command Attributes

- **Domain Lookup Status** – Enables DNS host name-to-address translation.
- **Default Domain Name*** – Defines the default domain name appended to incomplete host names. (Range: 1-64 alphanumeric characters)
- **Domain Name List*** – Defines define a list of domain names that can be appended to incomplete host names. (Range: 1-64 alphanumeric characters. 1-5 names)
- **Name Server List** – Specifies the address of one or more domain name servers to use for name-to-address resolution. (Range: 1-6 IP addresses)

* Do not include the initial dot that separates the host name from the domain name.

Downloaded from www.Manualslib.com manuals search engine

Web – Select DNS, General Configuration. Set the default domain name or list of domain names, specify one or more name servers to use to use for address resolution, enable domain lookup status, and click Apply.



Downloaded from www.Manualslib.com manuals search engine

CLI - This example sets a default domain name and a domain list. However, remember that if a domain list is specified, the default domain name is not used.

```
Console(config)#ip domain-name sample.com3-178
Console(config)#ip domain-list sample.com.uk3-179
Console(config)#ip domain-list sample.com.jp
Console(config)#ip domain-server 192.168.1.55 10.1.0.553-181
Console(config)#ip domain-lookup3-182
Console#show dns3-184
Domain Lookup Status:
    DNS enabled
Default Domain Name:
    .sample.com
Domain Name List:
    .sample.com.uk
    .sample.com.jp
Name Server List:
    192.168.1.55
    10.1.0.55
Console#
```

Configuring Static DNS Host to Address Entries

You can manually configure static entries in the DNS table that are used to map domain names to IP addresses.

Command Usage

- Static entries may be used for local devices connected directly to the attached network, or for commonly used resources located elsewhere on the network.

- Servers or other network devices may support one or more connections via multiple IP addresses. If more than one IP address is associated with a host name in the static table or via information returned from a name server, a DNS client can try each address in succession, until it establishes a connection with the target device.

Field Attributes

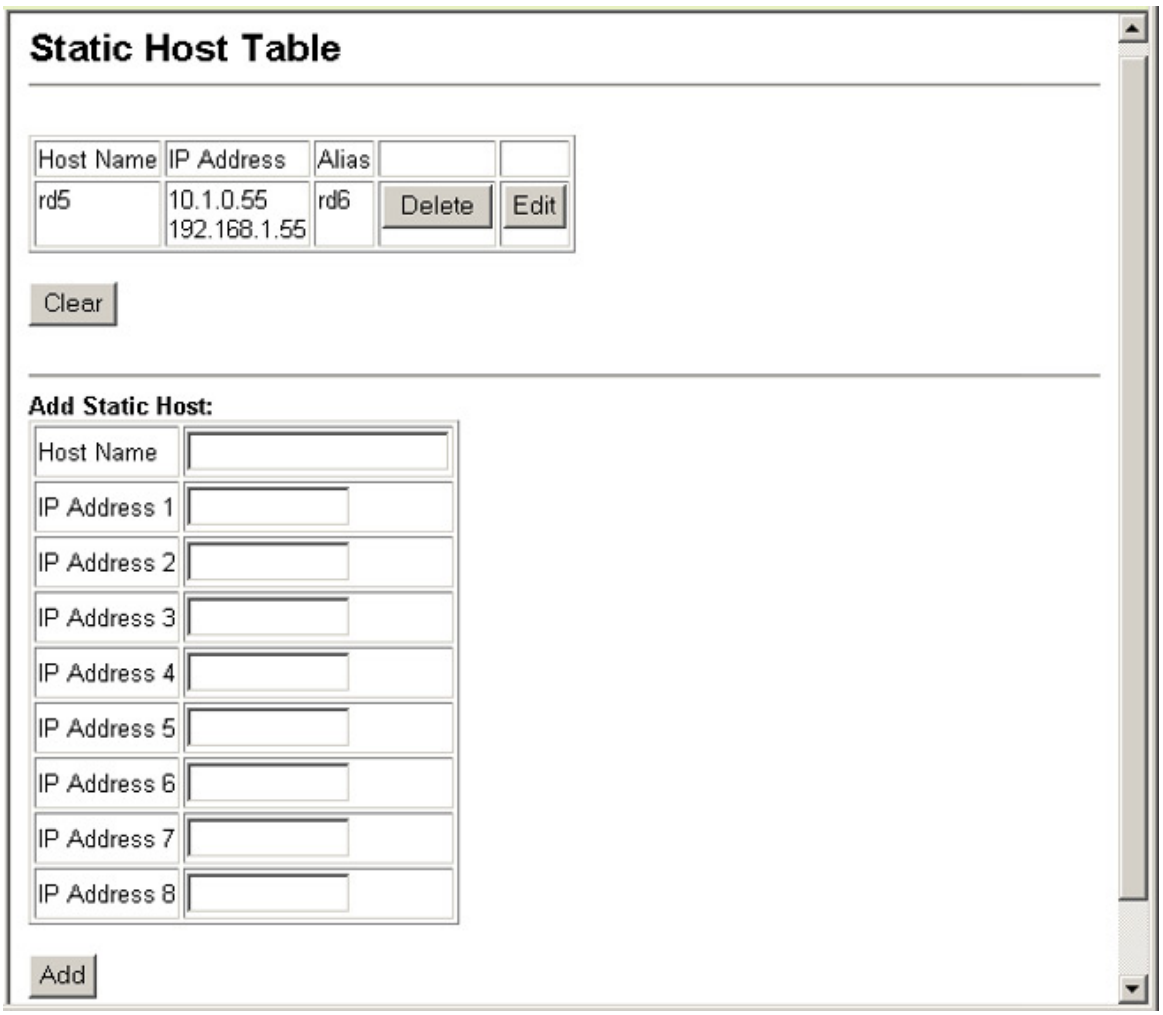
- **Host Name** – Name of a host device that is mapped to one or more IP addresses. (Range: 1-64 characters)

- **IP Address** – Internet address(es) associated with a host name. (Range: 1-8 addresses)

Downloaded from www.Manualslib.com manuals search engine

- **Alias** – Displays the host names that are mapped to the same address(es) as a previously configured entry.

Web – Select DNS, Static Host Table. Enter a host name and one or more corresponding addresses, then click Apply.



Downloaded from www.Manualslib.com manuals search engine

CLI - This example maps two address to a host name, and then configures an alias host name for the same addresses.

```
Console(config)#ip host rd5 192.168.1.55 10.1.0.553-177
Console(config)#ip host rd6 10.1.0.55
Console#show host3-183

Hostname
 rd5
Inet address
 10.1.0.55 192.168.1.55
Alias
 1.rd6
```


Downloaded from www.Manualslib.com manuals search engine

Displaying the DNS Cache

You can display entries in the DNS cache that have been learned via the designated name servers.

Field Attributes

- **No** – The entry number for each resource record.
- **Flag** – The flag is always "4" indicating a cache entry and therefore unreliable.
- **Type** – This field includes CNAME which specifies the canonical or primary name for the owner, and ALIAS which specifies multiple domain names which are mapped to the same IP address as an existing entry.
- **IP** – The IP address associated with this record.
- **TTL** – The time to live reported by the name server.
- **Domain** – The domain name associated with this record.

Web – Select DNS, Cache.

Cache

No	Flag	Type	IP	TTL	Domain
0	4	CNAME	207.46.134.222	51	www.microsoft.akadns.net
1	4	CNAME	207.46.134.190	51	www.microsoft.akadns.net
2	4	CNAME	207.46.134.155	51	www.microsoft.akadns.net
3	4	CNAME	207.46.249.222	51	www.microsoft.akadns.net
4	4	CNAME	207.46.249.27	51	www.microsoft.akadns.net
5	4	ALIAS	POINTER TO:4	51	www.microsoft.com
6	4	CNAME	207.46.68.27	71964	msn.com.tw
7	4	ALIAS	POINTER TO:6	71964	www.msn.com.tw
8	4	CNAME	65.54.131.192	605	passportimages.com
9	4	ALIAS	POINTER TO:8	605	www.passportimages.com
10	4	CNAME	165.193.72.190	87	global.msads.net

Downloaded from www.Manualslib.com manuals search engine

CLI - This example displays all the resource records learned from the designated name servers.

```
Console#show dns cache3-184
NO      FLAG    TYPE    IP              TTL     DOMAIN
0         4     CNAME   207.46.134.222  51      www.microsoft.akadns.net
1         4     CNAME   207.46.134.190  51      www.microsoft.akadns.net
2         4     CNAME   207.46.134.155  51      www.microsoft.akadns.net
3         4     CNAME   207.46.249.222  51      www.microsoft.akadns.net
4         4     CNAME   207.46.249.27   51      www.microsoft.akadns.net
5         4     ALIAS   POINTER TO:4    51      www.microsoft.com
6         4     CNAME   207.46.68.27    71964   msn.com.tw
7         4     ALIAS   POINTER TO:6    71964   www.msn.com.tw
8         4     CNAME   65.54.131.192   605     passportimages.com
9         4     ALIAS   POINTER TO:8    605     www.passportimages.com
10        4     CNAME   165.193.72.190  87      global.msads.net
Console#
```

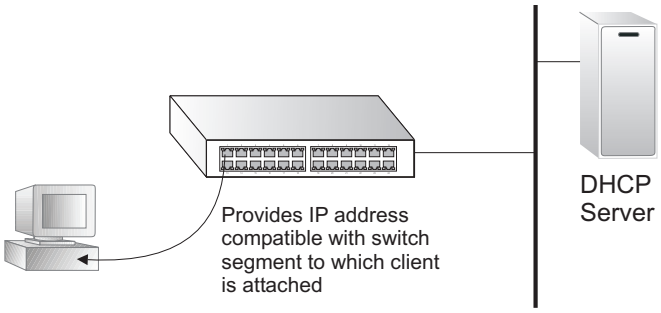
Dynamic Host Configuration Protocol

Dynamic Host Configuration Protocol (DHCP) can dynamically allocate an IP address and other configuration information to network clients when they boot up. If a subnet does not already include a BOOTP or DHCP server, you can relay DHCP client requests to a DHCP server on another subnet, or configure the DHCP server on this switch to support that subnet.

When configuring the DHCP server on this switch, you can configure an address pool for each unique IP interface, or manually assign a static IP address to clients based on their hardware address or client identifier. The DHCP server can provide the host's IP address, domain name, gateway router and DNS server, information about the host's boot image including the TFTP server to access for download and the name of the boot file, or boot information for NetBIOS Windows Internet Naming Service (WINS).

Downloaded from www.Manualslib.com manuals search engine

Configuring DHCP Relay Service



This switch supports DHCP relay service for attached host devices. If DHCP relay is enabled, and this switch sees a DHCP request broadcast, it inserts its own IP address into the request so that the DHCP server will know the subnet where the client is located. Then, the switch forwards the packet to the DHCP server. When the server receives the DHCP request, it allocates a free IP address for the DHCP client from its defined scope for the DHCP client's subnet, and sends a DHCP response back to the DHCP relay agent (i.e., this switch). This switch then broadcasts the DHCP response received from the server to the client.

Command Usage

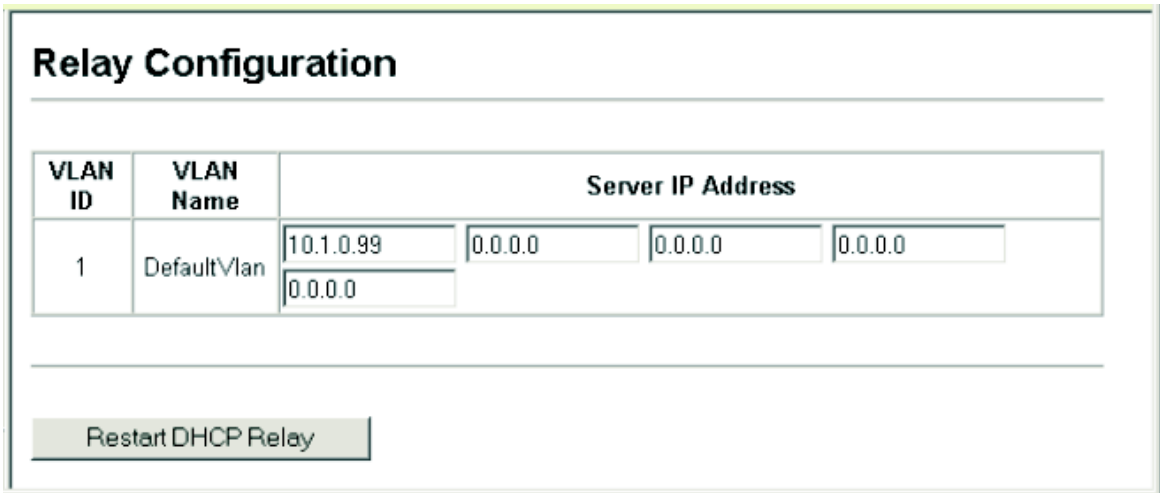
You must specify the IP address for at least one DHCP server. Otherwise, the switch's DHCP relay agent will not forward client requests to a DHCP server.

Command Attributes

- **VLAN ID** – ID of configured VLAN.
- **VLAN Name** – Name of the VLAN.
- **Server IP Address** – Addresses of DHCP servers to be used by the switch's DHCP relay agent in order of preference.

Downloaded from www.Manualslib.com manuals search engine

Web – Click DHCP, Relay Configuration. Enter up to five IP addresses for any VLAN, then click Restart DHCP Relay to start the relay service.



CLI – This example specifies one DHCP relay server for VLAN 1, and enables the relay service.

```
Console(config)#interface vlan 13-1
Console(config-if)#dhcp relay server 10.1.0.993-158
Console(config-if)#ip dhcp relay3-157
Console(config-if)#
```

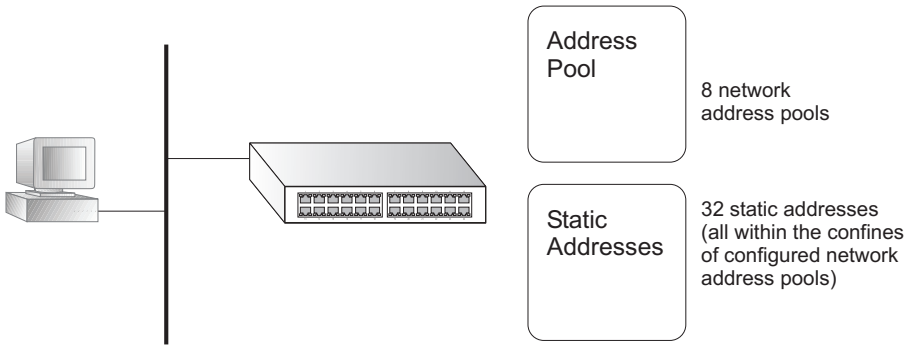
Configuring the DHCP Server

This switch includes a Dynamic Host Configuration Protocol (DHCP) server that can assign temporary IP addresses to any attached host requesting service. It can also provide other network settings such as the domain name, default gateway, Domain Name Servers (DNS), Windows Internet Naming Service (WINS) name servers, or information on the bootup file for the host device to download.

Addresses can be assigned to clients from a common address pool configured for a specific IP interface on this switch, or fixed addresses can

Downloaded from www.Manualslib.com manuals search engine

be assigned to hosts based on the client identifier code or MAC address.


Address Pool
8 network address pools
Static Addresses
32 static addresses (all within the confines of configured network address pools)

Command Usage

- First configure any excluded addresses, including the address for this switch.

- Then configure address pools for the network interfaces. You can configure up to 8 network address pools. You can also manually bind an address to a specific client if required. However, any fixed addresses must fall within the range of an existing network address pool. You can configure up to 32 fixed host addresses (i.e., entering one address per pool).

Enabling the Server, Setting Excluded Addresses

Enable the DHCP Server and specify the IP addresses that it should not be assigned to clients.

Command Attributes

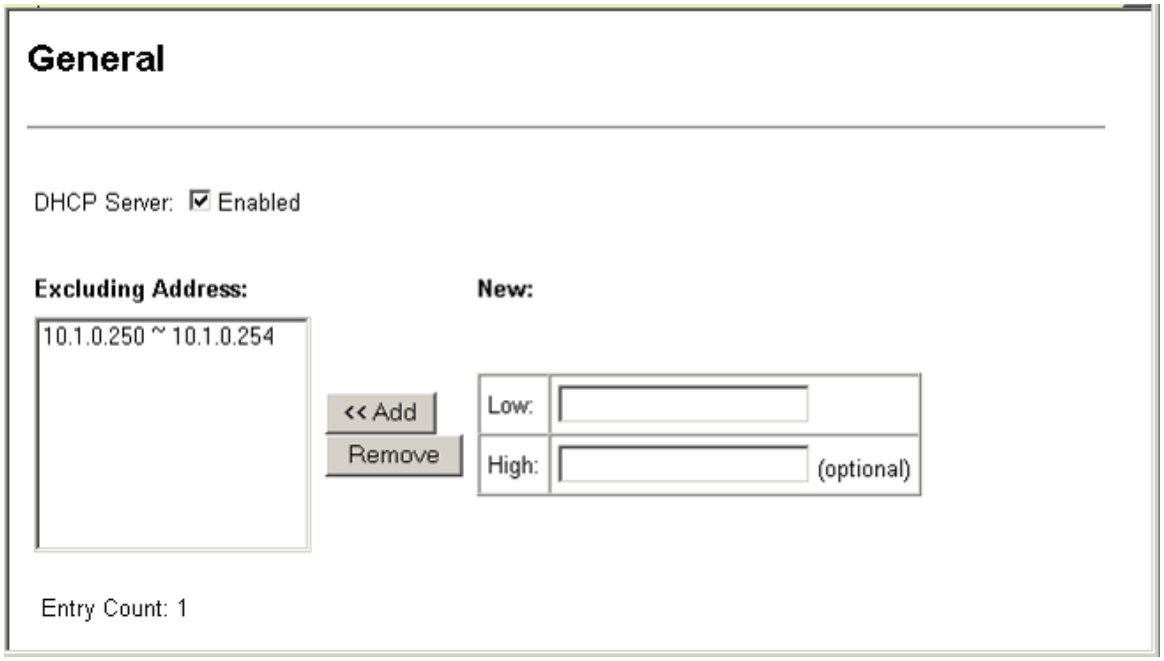
- **DHCP Server** – Enables or disables the DHCP server on this switch. (Default: Disabled)

- **Excluded Addresses** – Specifies IP addresses that the DHCP server should not assign to DHCP clients. You can specify a single address or an address range.

Note: Be sure you exclude the address for this switch and other key network devices.

Downloaded from www.Manualslib.com manuals search engine

Web – Click DHCP, Server, General. Enter a single address or an address range, and click Add.



CLI – This example enables the DHCP and sets an excluded address range.

```
Console(config)#service dhcp3-161
Console(config)#ip dhcp excluded-address 10.1.0.250 10.1.0.2543-161
Console#
```

Configuring Address Pools

You must configure IP address pools for each IP interface that will provide addresses to attached clients via the DHCP server.

Command Usage

- First configure address pools for the network interfaces. Then you can manually bind an address to a specific client if required. However, note that any static host address must fall within the range of an existing network address pool. You can configure up to 8 network address pools, and up to 32 manually bound host address pools (i.e., one address per host pool).

- When a client request is received, the switch first checks for a network

Downloaded from www.Manualslib.com manuals search engine

address pool matching the gateway where the request originated (i.e., if the request was forwarded by a relay server). If there is no gateway in the client request (i.e., the request was not forwarded by a relay server), the switch searches for a network pool matching the interface through which the client request was received. It then searches for a manually configured host address that falls within the matching network pool. If no manually configured host address is found, it assigns an address from the matching network address pool. However, if no matching address pool is found the request is ignored.

- When searching for a manual binding, the switch compares the client identifier and then the hardware address for DHCP clients. Since BOOTP clients cannot transmit a client identifier, you must configure a hardware address for this host type. If no manual binding has been specified for a host entry with a hardware address or client identifier, the switch will assign an address from the first matching network pool.

- If the subnet mask is not specified for network or host address pools, the class A, B, or C natural mask is used (see page 3-276). The DHCP server assumes that all host addresses are available. You can exclude subsets of the address space by using the IP Excluded Address field on the DHCP Server General configuration page.

Command Attributes

Creating a New Address Pool

- **Pool Name** – A string or integer. (Range: 1-8 characters)

Setting the Network Parameters

- **IP** – The IP address of the DHCP address pool.

- **Subnet Mask** – The bit combination that identifies the network (or subnet) and the host portion of the DHCP address pool.

Setting the Host Parameters

- **IP** – The IP address of the DHCP address pool.

Downloaded from www.Manualslib.com manuals search engine

- **Subnet Mask** – Specifies the network mask of the client.
- **Hardware Address** – Specifies the MAC address and protocol used on the client. (Options: Ethernet, IEEE802, FDDI; Default: Ethernet)
- **Client-Identifier** – A unique designation for the client device, either a text string (1-15 characters) or hexadecimal value.

Setting the Optional Parameters

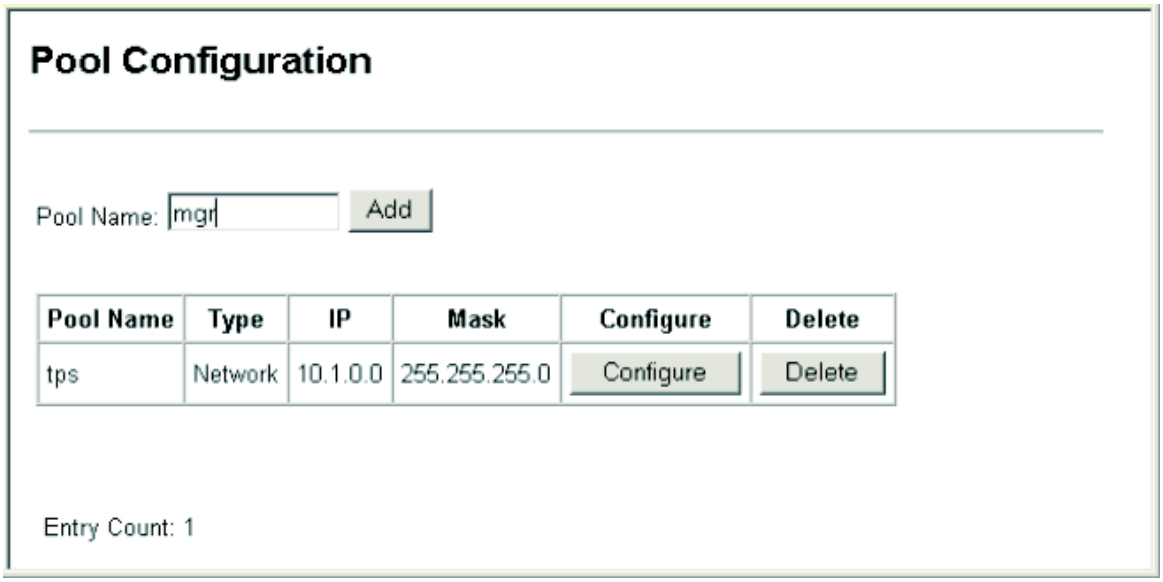
- **Default Router** – The IP address of the primary and alternate gateway router. The IP address of the router should be on the same subnet as the client.
- **DNS Server** – The IP address of the primary and alternate DNS server. DNS servers must be configured for a DHCP client to map host names to IP addresses.
- **Netbios Server** – IP address of the primary and alternate NetBIOS Windows Internet Naming Service (WINS) name server used for Microsoft DHCP clients.
- **Netbios Type** – NetBIOS node type for Microsoft DHCP clients. (Options: Broadcast, Hybrid, Mixed, Peer to Peer; Default: Hybrid)
- **Domain Name** – The domain name of the client. (Range: 1-32 characters)
- **Bootfile** – The default boot image for a DHCP client. This file should placed on the Trivial File Transfer Protocol (TFTP) server specified as the Next Server.
- **Next Server** – The IP address of the next server in the boot process, which is typically a Trivial File Transfer Protocol (TFTP) server.
- **Lease Time** – The duration that an IP address is assigned to a DHCP client. (Options: fixed period, Infinite; Default: 1 day)

Downloaded from www.Manualslib.com manuals search engine

Examples

Creating a New Address Pool

Web – Click DHCP, Server, Pool Configuration. Specify a pool name, then click Add.



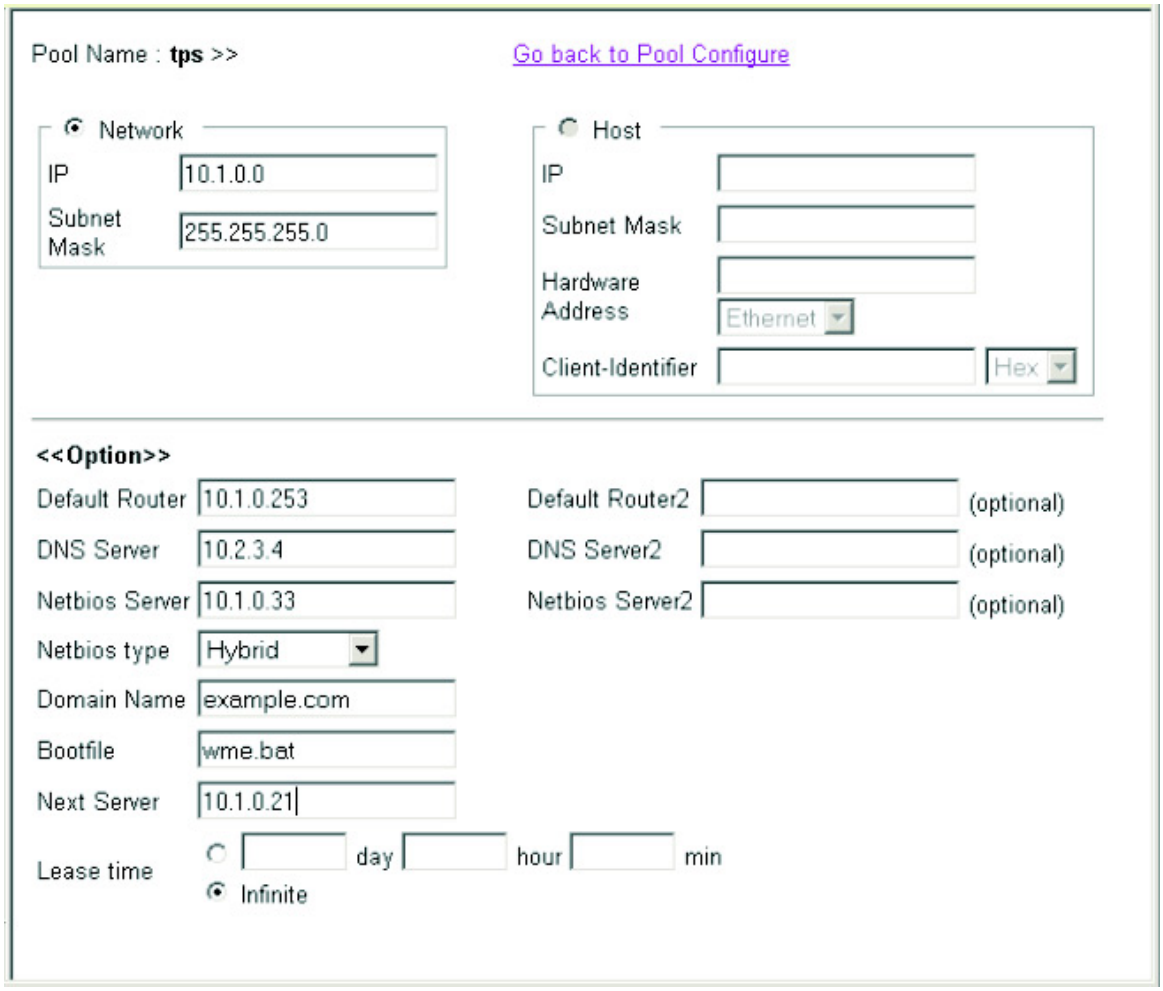
CLI – This example adds an address pool and enters DHCP pool configuration mode.

```
Console(config)#ip dhcp pool mgr3-162
Console(config-dhcp)#
```


Downloaded from www.Manualslib.com manuals search engine

Configuring a Network Address Pool

Web – Click DHCP, Server, Pool Configuration. Click the Configure button for any entry. Click the radio button for "Network." Enter the IP address and subnet mask for the network pool. Configure the optional parameters such as gateway server and DNS server. Then click Apply.



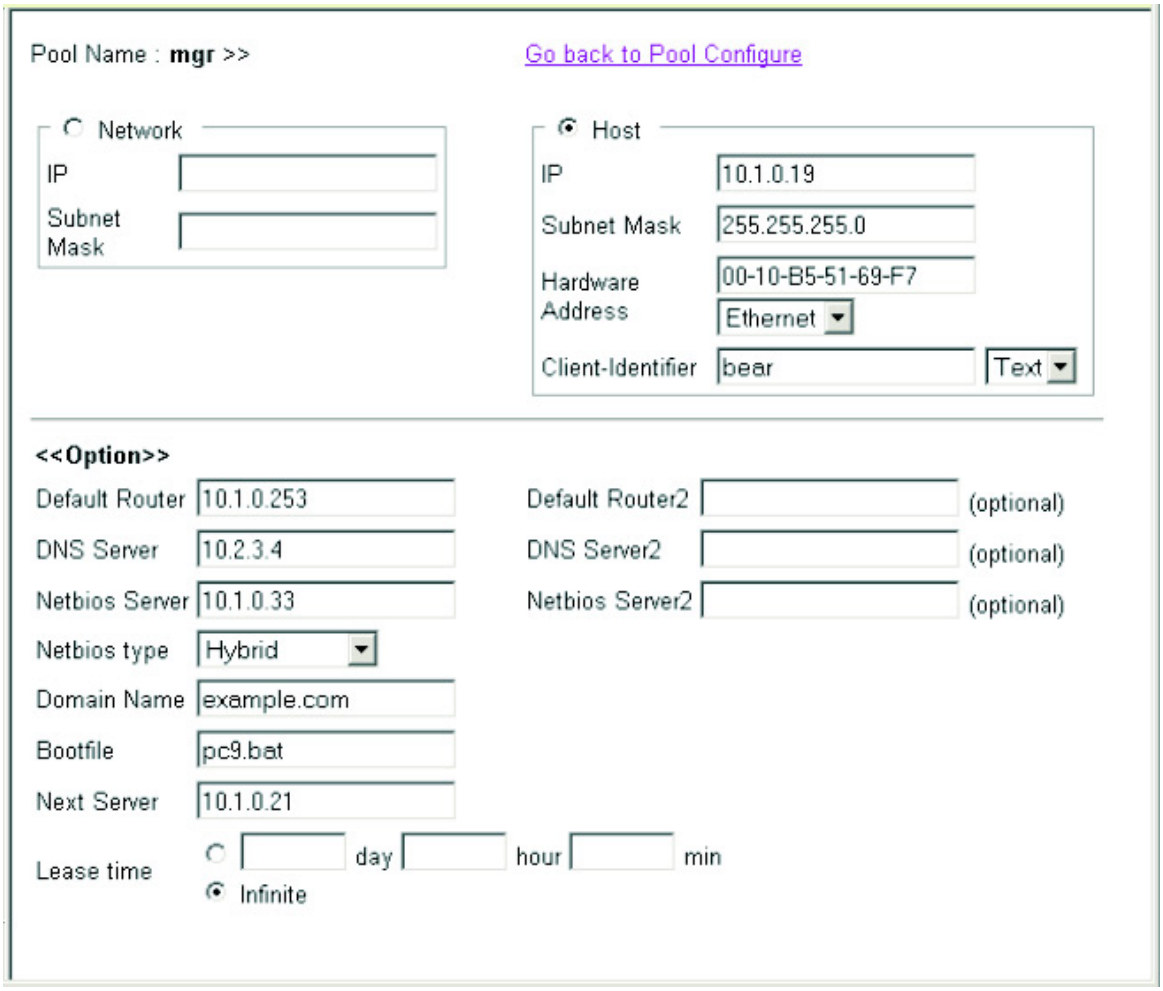
CLI – This example configures a network address pool.

```
Console(config)#ip dhcp pool tps3-162
Console(config-dhcp)#network 10.1.0.0 255.255.255.03-163
Console(config-dhcp)#default-router 10.1.0.2533-164
Console(config-dhcp)#dns-server 10.2.3.43-165
Console(config-dhcp)#netbios-name-server 10.1.0.333-167
Console(config-dhcp)#netbios-node-type hybrid3-168
Console(config-dhcp)#domain-name example.com3-165
Console(config-dhcp)#bootfile wme.bat3-167
Console(config-dhcp)#next-server 10.1.0.213-166
Console(config-dhcp)#lease infinite3-170
Console(config-dhcp)#
```


Downloaded from www.Manualslib.com manuals search engine

Configuring a Host Address Pool

Web – Click DHCP, Server, Pool Configuration. Click the Configure button for any entry. Click the radio button for "Host." Enter the IP address, subnet mask, and hardware address for the client device. Configure the optional parameters such as gateway server and DNS server. Then click Apply.



Downloaded from www.Manualslib.com manuals search engine

CLI – This example configures a host address pool.

```
Console(config)#ip dhcp pool mgr3-162
Console(config-dhcp)#host 10.1.0.19 255.255.255.03-170
Console(config-dhcp)#hardware-address 00-e0-29-94-34-28 ethernet3-173
Console(config-dhcp)#client-identifier text bear3-172
Console(config-dhcp)#default-router 10.1.0.2533-164
Console(config-dhcp)#dns-server 10.2.3.43-165
Console(config-dhcp)#netbios-name-server 10.1.0.333-167
Console(config-dhcp)#netbios-node-type hybrid3-168
Console(config-dhcp)#domain-name example.com3-165
Console(config-dhcp)#bootfile wme.bat3-167
Console(config-dhcp)#next-server 10.1.0.213-166
Console(config-dhcp)#lease infinite3-170
Console(config-dhcp)#
```

Displaying Address Bindings

You can display the host devices which have acquired an IP address from this switch's DHCP server.

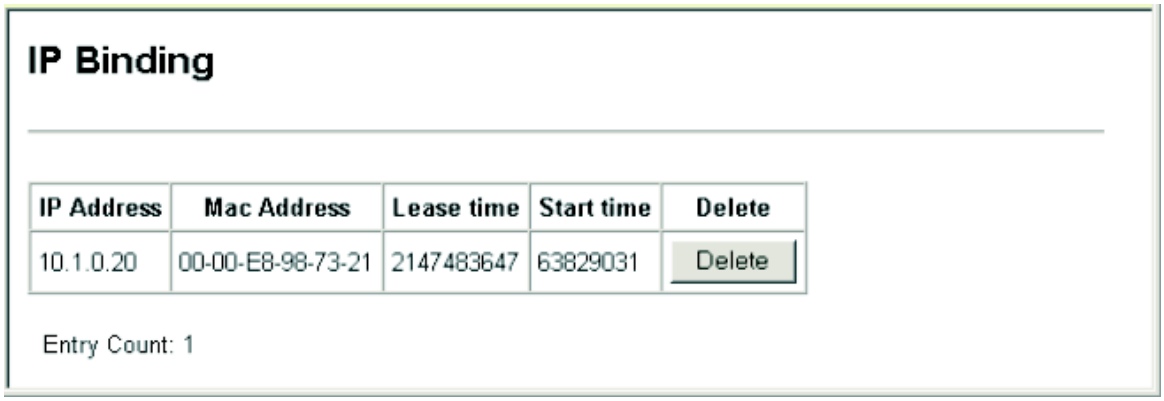
Command Attributes

- **IP Address** – IP address assigned to host.
- **Mac Address** – MAC address of host.
- **Lease time** – Duration that this IP address can be used by the host.
- **Start time** – Time this address was assigned by the switch.
- **Delete** – Clears this binding to the host. This command is normally used after modifying the address pool, or after moving DHCP service to another device.
- **Entry Count** – Number of hosts that have been given addresses by the switch.

Note: More than one DHCP server may respond to a service request by a host. In this case, the host generally accepts the first address assigned by any DHCP server.

Downloaded from www.Manualslib.com manuals search engine

Web – Click DHCP, Server, IP Binding. You may use the Delete button to clear an address from the DHCP server's database.



CLI – This example displays the current binding, and then clears all automatic binding.

```
Console#show ip dhcp binding3-175

     IP                MAC         Lease Time     Start
--------------- ----------------- ------------ -----------
     10.1.0.20 00-00-e8-98-73-21         86400 Dec 25 08:01:57 2002
Console#clear ip dhcp binding *3-174
Console#
```


Downloaded from www.Manualslib.com manuals search engine

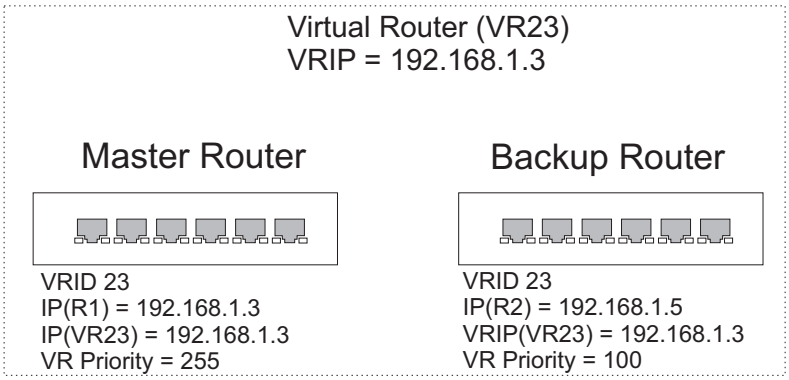
Configuring Router Redundancy

Router redundancy protocols use a virtual IP address to support a primary router and multiple backup routers. The backup routers can be configured to take over the workload if the master router fails, or can also be configured to share the traffic load. The primary goal of router redundancy is to allow a host device which has been configured with a fixed gateway to maintain network connectivity in case the primary gateway goes down.

This switch supports both the Virtual Router Redundancy Protocol (VRRP) and Hot Standby Router Protocol (HSRP). These protocols are very similar. The primary difference is that VRRP requires you to specify the interface of one of the routers participating in the virtual group as the address for the master virtual router, while HSRP requires you to configure an arbitrary address for the virtual master router. Both protocols then select the backup routers based on the specified virtual router priority. HSRP also includes the ability to dynamically modify the virtual router priority based on the operational state of other interfaces on the router.

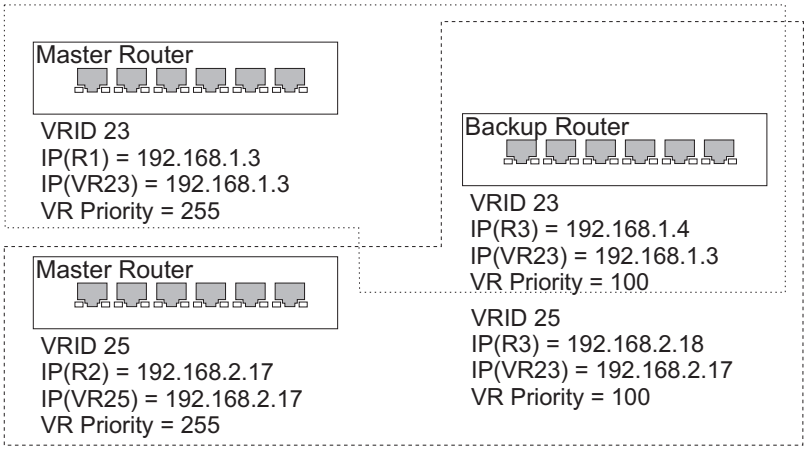
Router redundancy can be set up in any of the following configurations. The following examples show configuration settings for VRRP. The only difference for HSRP is that the virtual router IP address is never a real address, and the master router is selected based on priority only.

- A master virtual router with one or more backup routers.

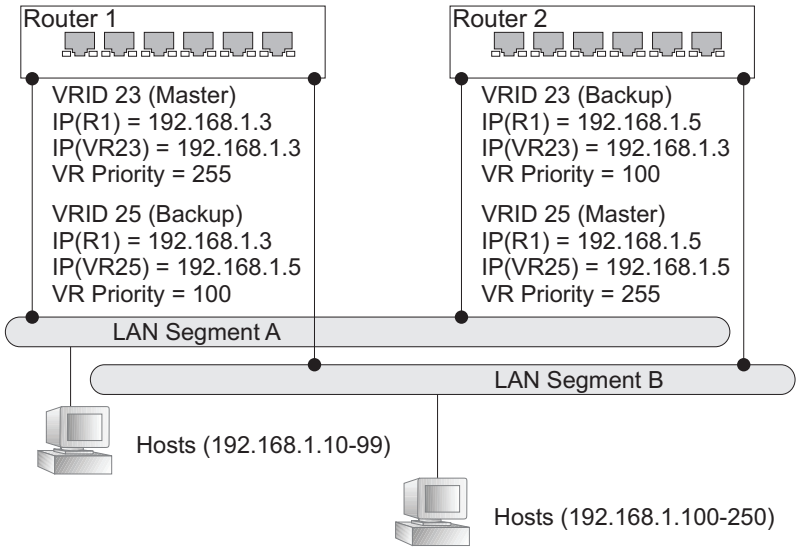


Downloaded from www.Manualslib.com manuals search engine

- Several virtual master routers using the same set of backup routers.



- Several virtual master routers configured for mutual backup and load sharing. Load sharing can be accomplished by assigning a subset of addresses to different host address pools using the DHCP server. (See "Configuring Address Pools" on page 3-217.)



Virtual Router Redundancy Protocol

Virtual Router Redundancy Protocol (VRRP) allows you to configure a group of routers as a single virtual router. The virtual router group is configured with a single virtual IP address that can be used as the default gateway for host devices on the attached network.

Downloaded from www.Manualslib.com manuals search engine

Configuring VRRP Groups

To configure VRRP, select an interface on one router in the group to serve as the master virtual router. This physical interface is used as the virtual address for the router group. Now set the same virtual address and a priority on the backup routers, and configure an authentication string. You can also enable the preempt feature which allows a router to take over as the master router when it comes on line.

Command Usage

Address Assignment –

- The IP address assigned to the virtual router must already be configured on the router that will be the Owner. In other words, the IP address for the virtual router exists on one, and only one, router in the virtual router group, and the network mask for the virtual router address is derived from the Owner. The Owner will also assume the role of the Master virtual router in the group.

- If you have multiple secondary addresses configured on the current VLAN interface, you can add any of these addresses to the virtual router group.

- The interfaces of all routers participating in a virtual router group must be within the same IP subnet.

- VRRP creates a virtual MAC address for the master router based on a standard prefix, with the last octet equal to the group ID. When a backup router takes over as the master, it continues to forward traffic addressed to this virtual MAC address. However, the backup router cannot reply to ICMP pings sent to addresses associated with the virtual group because the IP address owner is off line.

Virtual Router Priority –

- The Owner of the virtual IP address is automatically assigned the highest possible virtual router priority of 255. The backup router with the highest priority will become the master router if the current master

Downloaded from www.Manualslib.com manuals search engine

fails. However, because the priority of the virtual IP address Owner is the highest, the original master router will always become the active master router when it recovers.

- If two or more routers are configured with the same VRRP priority, the router with the higher IP address is elected as the new master router if the current master fails.

Preempting the Acting Master –

- The virtual IP Owner has the highest priority, so no other router can preempt it, and it will always resume control as the master virtual router when it comes back on line. The preempt function only allows a backup router to take over from another backup router that is temporarily acting as the group master. If preemption is enabled and this router has a higher priority than the current acting master when it comes on line, it will take over as the acting group master.

- You can add a delay to the preempt function to give additional time to receive an advertisement message from the current master before taking control. If the router attempting to become the master has just come on line, this delay also gives it time to gather information for its routing table before actually preempting the currently active master router.

Field Attributes (VRRP Group Configuration)

- **VLAN ID** – ID of a VLAN configured with an IP interface. (Range: 1-4094; Default: 1)

- **VRID** – VRRP group identifier. (Range: 1-255)

- **State** – VRRP router role. (Values: Master, Backup)

- **Virtual Address** – Virtual IP address for this group.

- **Interval** – Interval at which the master virtual router sends advertisements communicating its state as the master.

Downloaded from www.Manualslib.com manuals search engine

- **Preemption** – Shows if this router is allowed to preempt the acting master.
- **Priority** – Priority of this router in the VRRP group.
- **AuthType** – Authentication mode used to verify VRRP packets from other routers.

Downloaded from www.Manualslib.com manuals search engine

Command Attributes (VRRP Group Configuration Detail)

- **Associated IP Table** – IP interfaces associated with this virtual router group.

- **Associated IP** – IP address of the virtual router, or secondary IP addresses assigned to the current VLAN interface that are supported by this VRRP group. If this address matches a real interface on this switch, then this interface will become the virtual master router for this VRRP group.

- **Advertisement Interval** – Interval at which the master virtual router sends advertisements communicating its state as the master. (Range: 1-255 seconds; Default: 1 second)

  - VRRP advertisements from the current master virtual router include information about its priority and current state as the master.
  - VRRP advertisements are sent to the multicast address 224.0.0.8. Using a multicast address reduces the amount of traffic that has to be processed by network devices that are not part of the designated VRRP group.
  - If the master router stops sending advertisements, backup routers will bid to become the master router based on priority. The dead interval before attempting to take over as the master is three times the hello interval plus half a second.

- **Preempt Mode** – Allows a backup router to take over as the master virtual router if it has a higher priority than the acting master virtual router (i.e., another backup router that has taken over from the VRRP group address owner.) (Default: Enabled)

- **Preempt Delay** – Time to wait before issuing a claim to become the master. (Range: 0-120 seconds; 0 seconds)

- **Priority** – The priority of this router in a VRRP group. (Range: 1-254; Default: 100)

Downloaded from www.Manualslib.com manuals search engine

- The priority for the VRRP group address owner is automatically set to 255.
- The priority for backup routers is used to determine which router will take over as the acting master router if the current master fails.

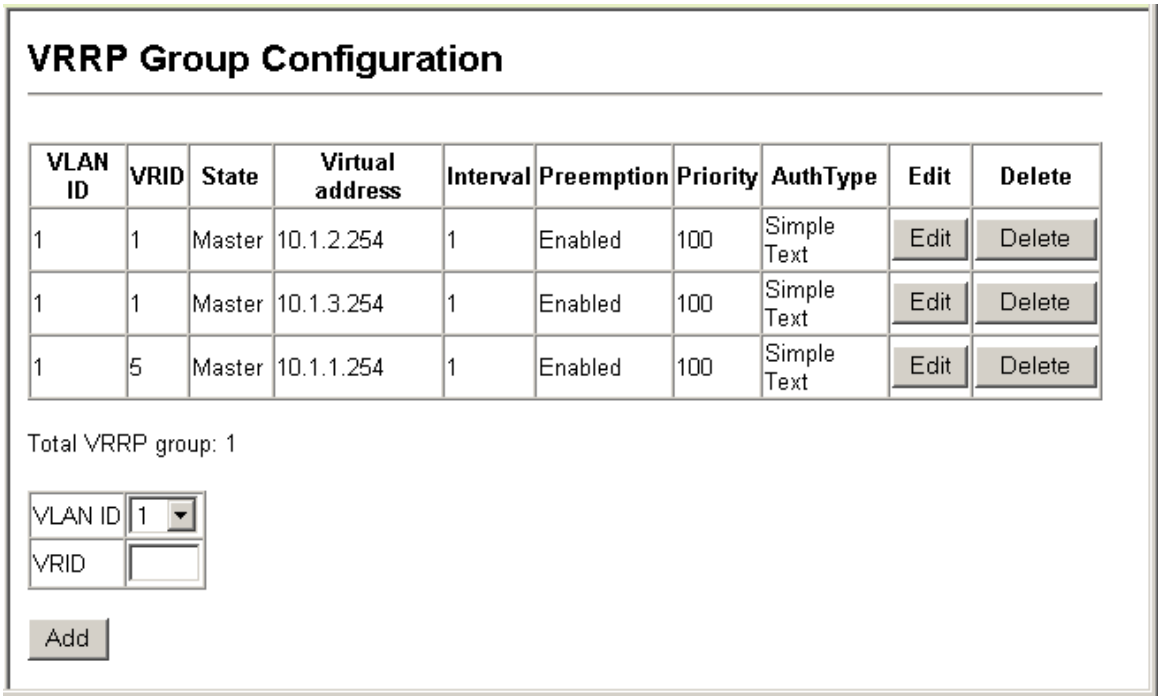
- **Authentication Type** – Authentication mode used to verify VRRP packets received from other routers. (Options: None, Simple Text)

  - If simple text authentication is selected, then you must also enter an authentication string.
  - All routers in the same VRRP group must be set to the same authentication mode, and be configured with the same authentication string.
  - Plain text authentication does not provide any real security. It is supported only to prevent a misconfigured router from participating in VRRP.
- **Authentication String** – Key used to authenticate VRRP packets received from other routers. (Range: 1-8 alphanumeric characters)

  - When a VRRP packet is received from another router in the group, its authentication string is compared to the string configured on this router. If the strings match, the message is accepted. Otherwise, the packet is discarded.

Downloaded from www.Manualslib.com manuals search engine

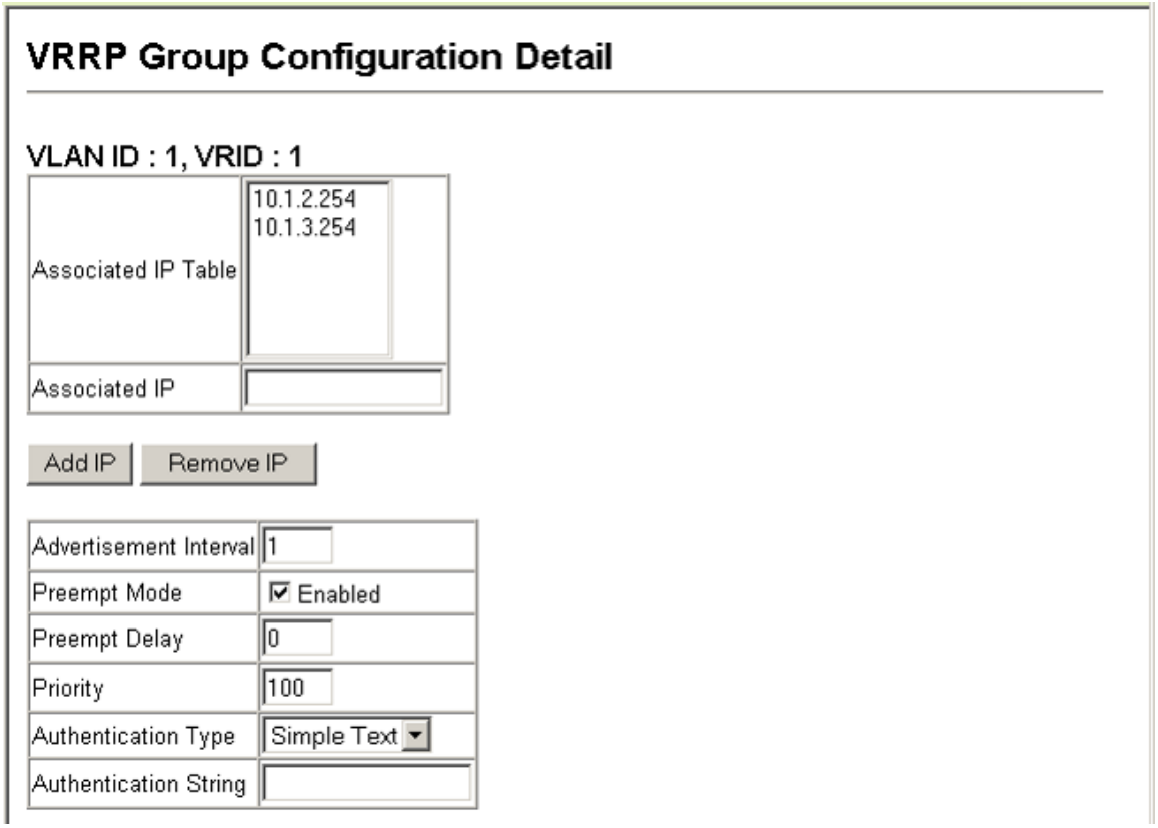
Web – Click IP, VRRP, Group Configuration. Select the VLAN ID, enter the VRID group number, and click Add.



Click the Edit button for a group entry to open the detailed configuration window. Enter the IP address of a real interface on this router to make it the master virtual router for the group. Otherwise, enter the virtual address for an existing group to make it a backup router. Click Add IP to enter an

Downloaded from www.Manualslib.com manuals search engine

IP address into the Associated IP Table. Then set any of the other parameters as required, and click Apply.



CLI – This example creates VRRP group 1, sets this switch as the master virtual router by assigning the primary interface address for the selected VLAN to the virtual IP address. It then adds a secondary IP address to the

Downloaded from www.Manualslib.com manuals search engine

VRRP group, sets all of the other VRRP parameters, and then displays the configured settings.

```
Console(config)#interface vlan 13-57
Console(config-if)#vrrp 1 ip 192.168.1.63-212
Console(config-if)#vrrp 1 ip 192.168.2.6 secondary
Console(config-if)#vrrp 1 timers advertise 53-216
Console(config-if)#vrrp 1 preempt delay 103-217
Console(config-if)#vrrp 1 priority 13-215
Console(config-if)#vrrp 1 authentication bluebird3-214
Console(config-if)#end
Console#show vrrp3-218
 Vlan 1 - Group 1,
 state                              Master
 Virtual IP address                 192.168.1.6
 Virtual MAC address                00-00-5E-00-01-01
 Advertisement interval             5 sec
 Preemption                         enabled
 Min delay                          10 sec
 Priority                           1
 Authentication                     SimpleText
 Authentication key                 bluebird
 Master Router                      192.168.1.6
 Master priority                    255
 Master Advertisement interval      5 sec
 Master down interval               15
Console#
```

Displaying VRRP Global Statistics

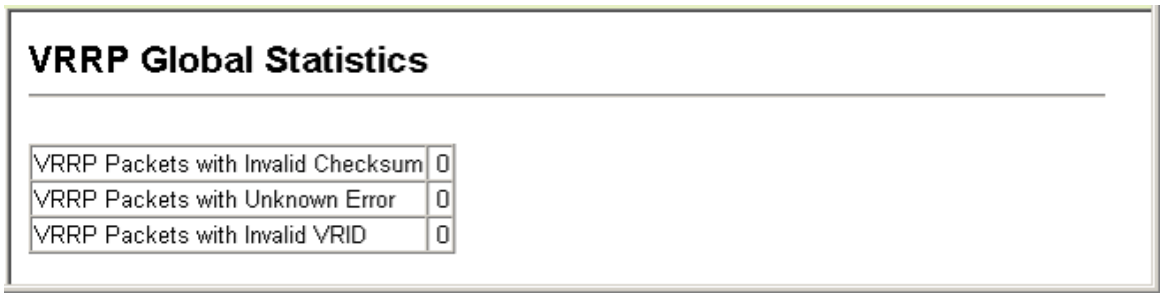
The VRRP Global Statistics page displays counters for errors found in VRRP protocol packets.

Field Attributes

- **VRRP Packets with Invalid Checksum** – The total number of VRRP packets received with an invalid VRRP checksum value.
- **VRRP Packets with Unknown Error** – The total number of VRRP packets received with an unknown or unsupported version number.
- **VRRP Packets with Invalid VRID** – The total number of VRRP packets received with an invalid VRID for this virtual router.

Downloaded from www.Manualslib.com manuals search engine

Web – Click IP, VRRP, Global Statistics.


VRRP Global Statistics
VRRP Packets with Invalid Checksum 0
VRRP Packets with Unknown Error 0
VRRP Packets with Invalid VRID 0

CLI – This example displays counters for protocol errors for all the VRRP groups configured on this switch.

```
Console#show vrrp router counters3-222
  VRRP Packets with Invalid Checksum : 0
  VRRP Packets with Unknown Error    : 0
  VRRP Packets with Invalid VRID     : 0
Console#
```

Displaying VRRP Group Statistics

The VRRP Group Statistics page displays counters for VRRP protocol events and errors that have occurred on a specific VRRP interface.

Field Attributes

- **VLAN ID** – ID of a VLAN configured with an IP interface. (Range: 1-4094; Default: 1)
- **VRID** – VRRP group identifier. (Range: 1-255)
- **Times Become Master** – Number of times this router has transitioned to master.
- **Received Packets** – Number of VRRP advertisements received by this router.
- **Error Interval Packets** – Number of VRRP advertisements received for which the advertisement interval is different from the one configured for the local virtual router.
- **Authentication Failures** – Number of VRRP packets received that do

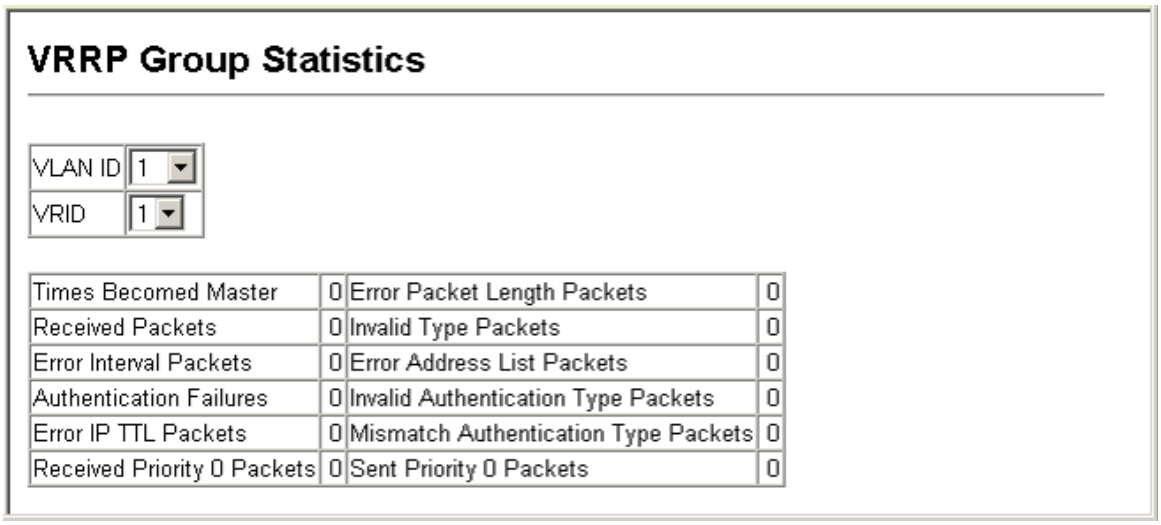
Downloaded from www.Manualslib.com manuals search engine

not pass the authentication check.

- **Error IP TTL Packets** – Number of VRRP packets received by the virtual router with IP TTL (Time-To-Live) not equal to 255.
- **Received Priority 0 Packets** – Number of VRRP packets received by the virtual router with priority set to 0.
- **Error Packet Length Packets** – Number of packets received with a packet length less than the length of the VRRP header.
- **Invalid Type Packets** – Number of VRRP packets received by the virtual router with an invalid value in the "type" field.
- **Error Address List Packets** – Number of packets received for which the address list does not match the locally configured list for the virtual router.
- **Invalid Authentication Type Packets** – Number of packets received with an unknown authentication type.
- **Mismatch Authentication Type Packets** – Number of packets received with "Auth Type" not equal to the locally configured authentication method.
- **Sent Priority 0 Packets** – Number of VRRP packets sent by the virtual router with priority set to 0.

Downloaded from www.Manualslib.com manuals search engine

Web – Click IP, VRRP, Group Statistics. Select the VLAN and virtual router group.



VRRP Group Statistics

VLAN ID 1
VRID 1

Times Becomed Master	0	Error Packet Length Packets	0
Received Packets	0	Invalid Type Packets	0
Error Interval Packets	0	Error Address List Packets	0
Authentication Failures	0	Invalid Authentication Type Packets	0
Error IP TTL Packets	0	Mismatch Authentication Type Packets	0
Received Priority 0 Packets	0	Sent Priority 0 Packets	0

CLI – This example displays VRRP protocol statistics for group 1, VLAN 1.

```
Console#show vrrp 1 interface vlan 1 counters3-222
 Total Number of Times Transitioned to MASTER                        : 6
 Total Number of Received Advertisements Packets                     : 0
 Total Number of Received Error Advertisement Interval Packets       : 0
 Total Number of Received Authentication Failures Packets            : 0
 Total Number of Received Error IP TTL VRRP Packets                  : 0
 Total Number of Received Priority 0 VRRP Packets                    : 0
 Total Number of Sent Priority 0 VRRP Packets                        : 5
 Total Number of Received Invalid Type VRRP Packets                  : 0
 Total Number of Received Error Address List VRRP Packets            : 0
 Total Number of Received Invalid Authentication Type VRRP Packets   : 0
 Total Number of Received Mismatch Authentication Type VRRP Packets  : 0
 Total Number of Received Error Packet Length VRRP Packets           : 0
Console#
```

Hot Standby Router Protocol

Hot Standby Router Protocol (HSRP) allows you to configure a group of routers as a single virtual router. The virtual router group is configured with a single virtual IP address that can be used as the default gateway for host devices on the attached network.

Downloaded from www.Manualslib.com manuals search engine

Configuring HSRP Groups

To configure HSRP, assign the same virtual router address to each router in the group. Set the highest virtual router priority on the router that will serve as the master. Enable the preempt feature to allow a router to take over as the master when it comes on line (if it has a higher priority). To configure the backup routers with an order of precedence for assuming the role of master, set the appropriate priority on each of these routers.Then configure an authentication string to ensure that HSRP messages are only be exchanged between authorized routers. You can also dynamically adjust the virtual router priority by tracking the availability of any IP interfaces on the router.

Command Usage

Address Assignment –

- The designated virtual IP address must be configured on at least one router in the virtual router group. If an IP address is not specified, the designated address is learned through the exchange of HSRP messages. Note that the designated address cannot be the same as a physical address.

- The subnet mask for the physical interface on which the designated address is configured is used as the subnet mask of the designated address. The interfaces of all routers participating in a virtual router group must be within the same IP subnet.

- Configuring a new designated address on the current master router will override the designated address currently is use.

- If multiple secondary addresses are configured on the current VLAN interface, these addresses can also be supported on the virtual router by selecting the "Secondary" Virtual IP mode.

- HSRP is enabled once the designated address and priority are configured, and the master and standby routers are elected based on highest priority. If you need to customize any of the other parameters

Downloaded from www.Manualslib.com manuals search engine

for HSRP such as authentication, tracking, or advertisement interval, then first configure these parameters before enabling HSRP.

- HSRP creates a virtual MAC address for the master router based on a standard prefix, with the last octet equal to the group ID. When a backup router takes over as the master, it continues to forward traffic addressed to this virtual MAC address. However, the backup router cannot reply to ICMP pings sent to addresses associated with the virtual group because the IP address owner is off line.

Virtual Router Priority –

- The router with the highest priority is elected as the master virtual router. The router with the next highest priority is elected as the standby router. The standby router will become the master router if the current master fails. When the original master router recovers, it will become the active master router again if the configured priorities have not been changed.

- If two or more routers are configured with the same HSRP priority, the router with the higher IP address is elected as the new master router if the current master fails.

- The priority setting takes precedence over authentication. In other words, if a router with a higher priority than any other router comes on line, but is not configured with an authentication string, or is configured with the wrong string, it will still take over as the active master.

- The HSRP priority can change dynamically depending on the availability of a tracked interface.

Preempting the Master –

- If preempt is enabled, and this router has a priority higher than the current acting master, it will take over as the new master. If preempt is not enabled, this router will only take over if it has the highest priority in the group and the current master stops sending hello messages or

Downloaded from www.Manualslib.com manuals search engine

sends other messages indicating that it is no longer acting as the designated router.

- You can add a delay to the preempt function to give additional time to receive an advertisement message from the current master before taking control. If the router attempting to become the master has just come on line, this delay also gives it time to gather information for its routing table before actually preempting the currently active master router.

Field Attributes (HSRP Group Configuration)

- **VLAN ID** – ID of a VLAN configured with an IP interface. (Range: 1-4094; Default: 1)
- **Group** – HSRP group identifier. (Range: 1-255)
- **State** – HSRP router role. (Values: Master, Backup)
- **Virtual Address** – Virtual IP address for this group.
- **Hellotime** – Interval at which the master and standby virtual routers send advertisements communicating their state.
- **Holdtime** – Time before the master or standby router is declared down.
- **Preemption** – Shows if this router is allowed to preempt the acting master.
- **Priority** – Priority of this router in the HSRP group.

Command Attributes (HSRP Group Configuration Detail)

- **Hellotime** – Interval at which the master and standby virtual routers send advertisements communicating their state.
  (Range: 1-254 seconds; Default: 3)

Downloaded from www.Manualslib.com manuals search engine

- HSRP advertisements from the master and standby virtual router include information about their priority, timer values, and current state as the master or standby router.
- Routers on which the timer settings have not been configured can learn the current timer values from the master or standby router. Timers configured on the master router always override any other timer settings. All routers in an HSRP group should be configured with the same timer values.
- HSRP advertisements are sent to the multicast address 224.0.0.2. Using a multicast address reduces the amount of traffic that has to processed by network devices that are not part of the designated HSRP group.

- **Holdtime** – Time before the master or standby router is declared down. (Range: Hellotime+1 to 255 seconds; Default: 10 seconds)

  - If the master router stops sending advertisements, backup routers will bid to become the master based on priority. The hold time before declaring a router dead should be normally be set to a value 3 times or more than the hello time.

- **Preempt Mode** – Allows a backup router to take over as the master virtual router if it has a higher priority than the acting master virtual router. (Default: Disabled)

- **Preempt Delay** – Time to wait before issuing a claim to become the master. (Range: 0-3600 seconds; 0 seconds)

- **Priority** – Priority of this router in an HSRP group. (Range: 1-255; Default: 100)

- **Authentication String** – Key used to authenticate HSRP packets received from other routers. (Range: 1-8 alphanumeric characters)

  - All routers in the same HSRP group must be configured with the same authentication string. When a HSRP packet is received from another router in the group, its authentication string is compared

Downloaded from www.Manualslib.com manuals search engine

to the string configured on this router. If the strings match, the message is accepted. Otherwise, the packet is discarded.
- Plain text authentication does not provide any real security. It is supported only to prevent a misconfigured router from participating in HSRP.

- **Virtual IP** – IP address of the virtual router, or secondary IP addresses assigned to the current VLAN interface that are supported by the HSRP group.

- **Mode** – Sets this entry as the virtual IP address for the HSRP group (i.e., Primary), or as a secondary IP addresses assigned to the current VLAN interface that is also supported by the HSRP group. (Range: Primary, Secondary: Default: Primary)

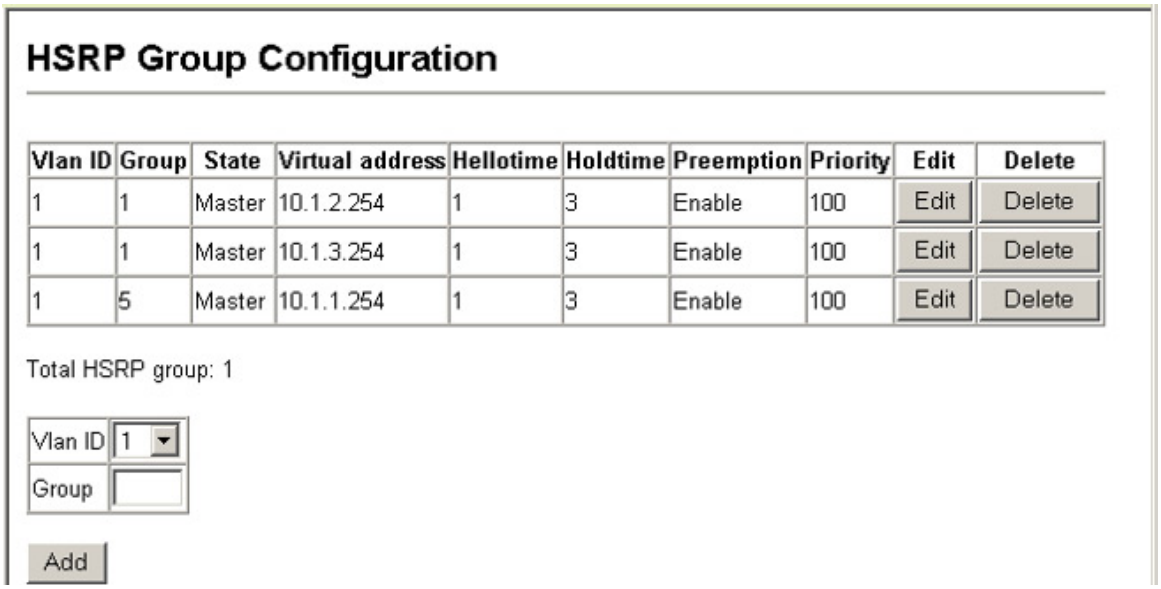
- **Tracking Interface** – Specifies an interface to track. The HSRP priority of this router will be changed whenever the interface goes down or comes back up by the corresponding tracking priority.

  - You can specify up to 32 IP interfaces to be tracked by this command.
  - If you specify a VLAN interface that has not been configured with an IP address, tracking will not affect the HSRP router priority.
- (Tracking) **Priority** – Amount by which the HSRP router priority is decremented (or incremented) when the interface goes down (or comes back up). (Range: 1-255; Default: 10)

  - If you configure multiple tracked interfaces, and also set the interface priority, the effect on HSRP router priority is cumulative when one or more interfaces go up or down. However, if you configure multiple tracked interfaces, but do not set the interface priority, HSRP router priority will only be changed by the default interface priority value of 10; i.e., the effect is not cumulative.

Web – Click IP, HSRP, Group Configuration. Select the VLAN ID, enter the HSRP group number, and click Add.

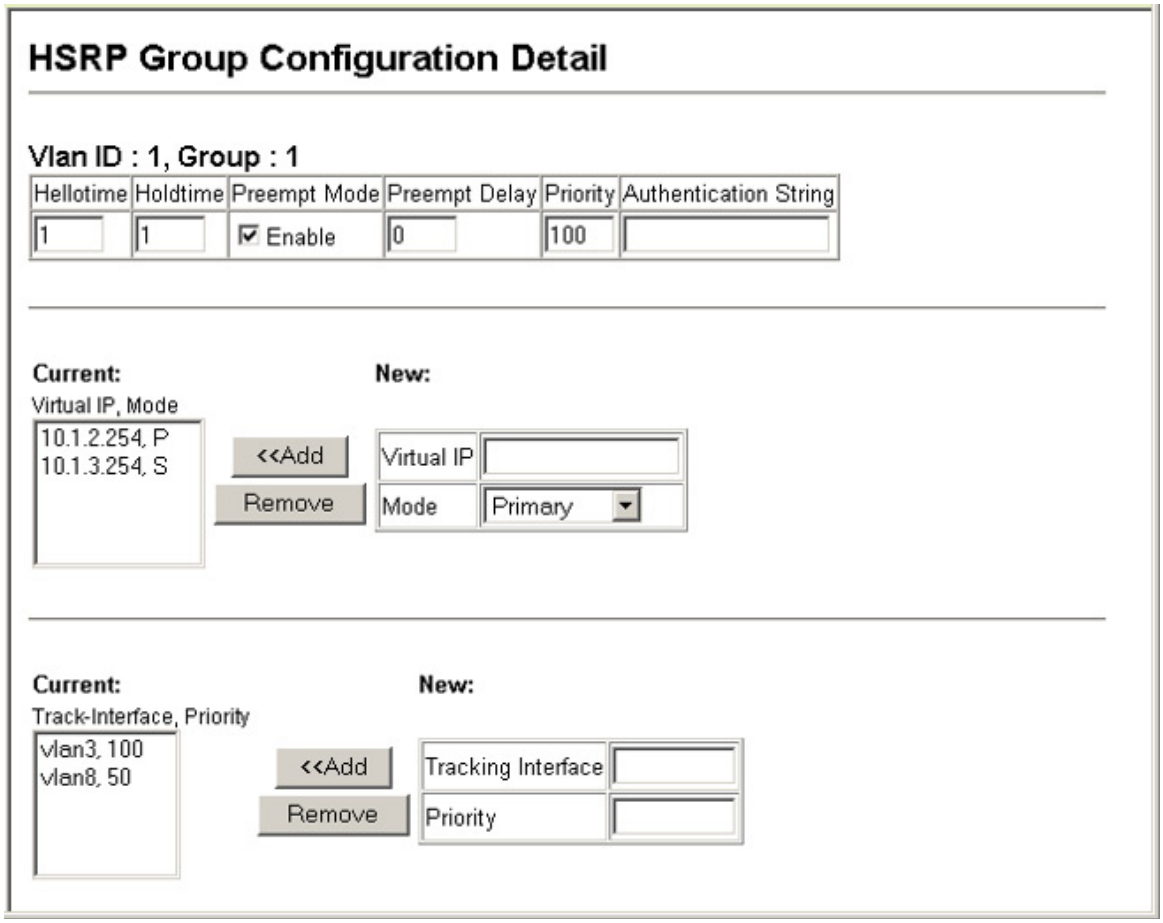
Downloaded from www.Manualslib.com manuals search engine


HSRP Group Configuration
Vlan ID Group State Virtual address Hellotime Holdtime Preemption Priority Edit Delete
1 1 Master 10.1.2.254 1 3 Enable 100 Edit Delete
1 1 Master 10.1.3.254 1 3 Enable 100 Edit Delete
1 5 Master 10.1.1.254 1 3 Enable 100 Edit Delete
Total HSRP group: 1
Vlan ID 1
Group
Add

Click the Edit button for a group entry to open the detailed configuration window. Set the values for the advertisement interval, preemption, priority, and authentication as required. Enter the virtual IP address for the group. You can also enter secondary IP addresses that will be supported by the group. Enter any IP interfaces for which the status should be tracked, and

Downloaded from www.Manualslib.com manuals search engine

the corresponding value by which to adjust the priority when the interface state changes. Then click Apply.



Downloaded from www.Manualslib.com manuals search engine

CLI – This example creates HSRP group 1, sets the virtual router's address, adds a secondary IP address to the group, specifies an interface for tracking, sets all the other HSRP parameters, and then displays the configured settings.

```
Console(config)#interface vlan 1
Console(config-if)#standby 1 ip 192.168.1.7
Console(config-if)#standby 1 ip 192.168.2.6 secondary
Console(config-if)#standby 1 track vlan 3 100
Console(config-if)#standby 1 timers 2 5
Console(config-if)#standby 1 preempt delay 10
Console(config-if)#standby 1 priority 10
Console(config-if)#standby 1 authentication bluebird
Console#show standby
Vlan 1 - Group 1
Local State is Active, priority 5 (confgd 10), may preempt
Preemption delayed for 10 secs
Hellotime 6 sec, holdtime 18 sec
Next hello sent in 0: 0: 5
Host standby IP address is 192.168.1.7 configured
Active router is local
Standby router is unknown
Standby virtual mac address is  0- 0- C- 7-AC- 1
Authentication text "bluebird"
Tracking interface states for 1 interfaces, 0 up
   Down    Vlan2     5
Console#
```


Downloaded from www.Manualslib.com manuals search engine

IP Routing

Overview

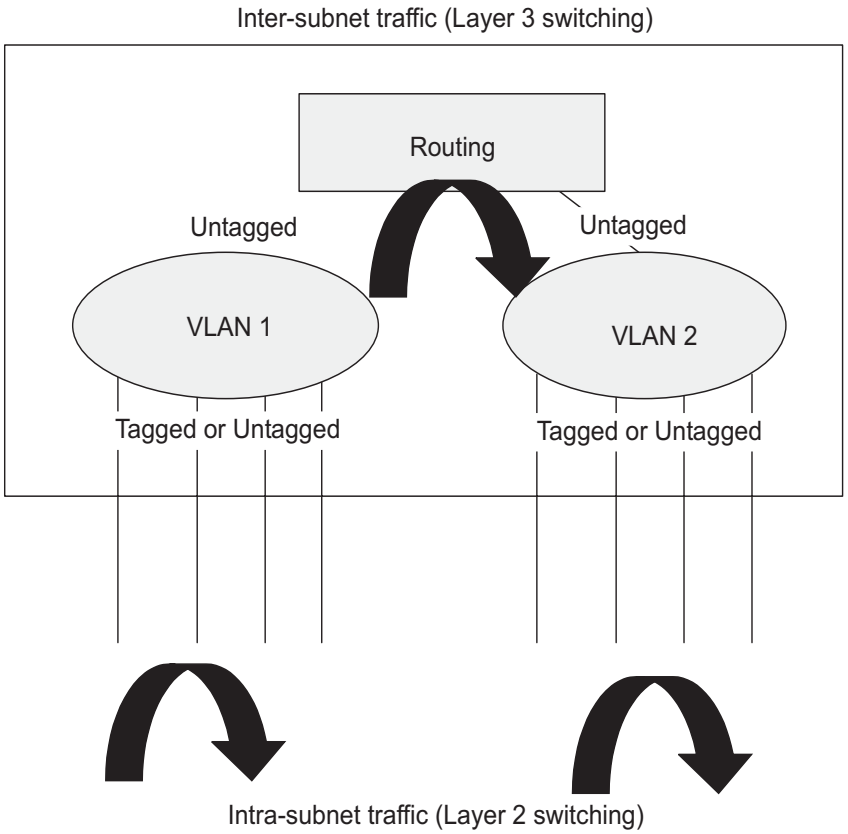
This switch supports IP routing and routing path management via static routing definitions (page 3-269) and dynamic routing such as RIP (page 3-273) or OSPF (page 3-285). When IP routing is enabled (page 3-274), this switch acts as a wire-speed router, passing traffic between VLANs using different IP interfaces, and routing traffic to external IP networks. However, when the switch is first booted, no default routing is defined. As with all traditional routers, the routing functions must first be configured to work.

Initial Configuration

In the default configuration, all ports belong to the same VLAN and the switch provides only Layer 2 functionality. Therefore, you should first create VLANs for each unique user group or application traffic (page 3-158), assign all ports that belong to the same group to these VLANs (page 3-159), and then assign an IP interface to each VLAN (page 3-252). By separating the network into different VLANs, it can be partitioned into subnetworks that are disconnected at Layer 2. Network traffic within the same subnet is still switched using Layer 2 switching. And the VLANs can now be interconnected (only as required) with Layer 3 switching.

Each VLAN represents a virtual interface to Layer 3. You just need to provide the network address for each virtual interface, and the traffic between different subnetworks will be routed by Layer 3 switching.

Downloaded from www.Manualslib.com manuals search engine



IP Switching

IP Switching (or packet forwarding) encompasses tasks required to forward packets for both Layer 2 and Layer 3, as well as traditional routing. These functions include:

- Layer 2 forwarding (switching) based on the Layer 2 destination MAC address
- Layer 3 forwarding (routing):

- Based on the Layer 3 destination address
- Replacing destination/source MAC addresses for each hop
- Incrementing the hop count
- Decrementing the time-to-live
- Verifying and recalculating the Layer 3 checksum

If the destination node is on the same subnetwork as the source network, then the packet can be transmitted directly without the help of a router.

Downloaded from www.Manualslib.com manuals search engine

However, if the MAC address is not yet known to the switch, an Address Resolution Protocol (ARP) packet with the destination IP address is broadcast to get the destination MAC address from the destination node. The IP packet can then be sent directly with the destination MAC address.

If the destination belongs to a different subnet on this switch, the packet can be routed directly to the destination node. However, if the packet belongs to a subnet not included on this switch, then the packet should be sent to a router (with the MAC address of the router itself used as the destination MAC address, and the destination IP address of the destination node). The router will then forward the packet to the destination node via the correct path. The router can also use the ARP protocol to find out the MAC address of the destination node of the next router as necessary.

Note: In order to perform IP switching, the switch should be recognized by other network nodes as an IP router, either by setting it as the default gateway or by redirection from another router via the ICMP process.

When the switch receives an IP packet addressed to its own MAC address, the packet follows the Layer 3 routing process. The destination IP address is checked against the Layer 3 address table. If the address is not already there, the switch broadcasts an ARP packet to all the ports on the destination VLAN to find out the destination MAC address. After the MAC address is discovered, the packet is reformatted and sent out to the destination. The reformat process includes decreasing the Time-To-Live (TTL) field of the IP header, recalculating the IP header checksum, and replacing the destination MAC address with either the MAC address of the destination node or that of the next hop router.

When another packet destined to the same node arrives, the destination MAC can be retrieved directly from the Layer 3 address table; the packet is then reformatted and sent out the destination port. IP switching can be done at wire-speed when the destination address entry is already in the Layer 3 address table.

If the switch determines that a frame must be routed, the route is

Downloaded from www.Manualslib.com manuals search engine

calculated only during setup. Once the route has been determined, all packets in the current flow are simply switched or forwarded across the chosen path. This takes advantage of the high throughput and low latency of switching by enabling the traffic to bypass the routing engine once the path calculation has been performed.

Routing Path Management

Routing Path Management involves the determination and updating of all the routing information required for packet forwarding, including:

- Handling routing protocols
- Updating the routing table
- Updating the Layer 3 switching database

Routing Protocols

The switch supports both static and dynamic routing.

- Static routing requires routing information to be stored in the switch either manually or when a connection is set up by an application outside the switch.
- Dynamic routing uses a routing protocol to exchange routing information, calculate routing tables, and respond to changes in the status or loading of the network.

The switch supports RIP, RIP-2 and OSPFv2 dynamic routing protocols.

RIP and RIP-2 Dynamic Routing Protocols

The RIP protocol is the most widely used routing protocol. RIP uses a distance-vector-based approach to routing. Routes are determined on the basis of minimizing the distance vector, or hop count, which serves as a rough estimate of transmission cost. Each router broadcasts its advertisement every 30 seconds, together with any updates to its routing table. This allows all routers on the network to learn consistent tables of next hop links which lead to relevant subnets.

Downloaded from www.Manualslib.com manuals search engine

OSPFv2 Dynamic Routing Protocol

OSPF overcomes all the problems of RIP. It uses a link state routing protocol to generate a shortest-path tree, then builds up its routing table based on this tree. OSPF produces a more stable network because the participating routers act on network changes predictably and simultaneously, converging on the best route more quickly than RIP. Moreover, when several equal-cost routes to a destination exist, traffic can be distributed equally among them.

Non-IP Protocol Routing

The switch supports IP routing only. Non-IP protocols such as IPX and Appletalk cannot be routed by this switch, and will be confined within their local VLAN group unless bridged by an external router.

To coexist with a network built on multilayer switches, the subnetworks for non-IP protocols must follow the same logical boundary as that of the IP subnetworks. A separate multi-protocol router can then be used to link the subnetworks by connecting to one port from each available VLAN on the network.

Basic IP Interface Configuration

To allow routing between different IP subnets, you must enable IP Routing as described in this section. You also need to you define a VLAN for each IP subnet that will be connected directly to this switch. Note that you must first create a VLAN as described under "Creating VLANs" on page 3-158 before configuring the corresponding subnet. Remember that if you need to manage the switch in-band then you must define the IP subnet address for at least one VLAN.

Command Attributes

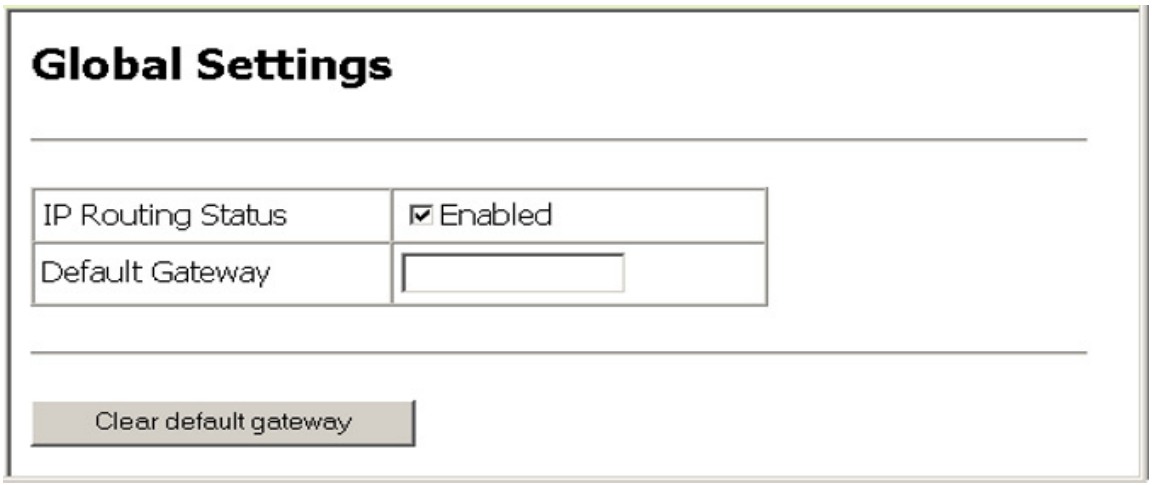
- **IP Routing Status** – Configures the switch to operate as a Layer 2 switch or as a multilayer routing switch. (Options: Disable this field to restrict operation to Layer 2 switching; enable it to allow multilayer operation at either Layer 2 or 3 as required.)

Downloaded from www.Manualslib.com manuals search engine

- This command affects both static and dynamic unicast routing.
- If IP routing is enabled, all IP packets are routed using either static routing or dynamic routing via RIP or OSPF, and other packets for all non-IP protocols (e.g., NetBuei, NetWare or AppleTalk) are switched based on MAC addresses. If IP routing is disabled, all packets are switched, with filtering and forwarding decisions based strictly on MAC addresses.

- **Default Gateway** – The routing device to which the switch will pass packets for all unknown subnets; i.e., packets that do not match any routing table entry. (Valid IP addresses consist of four numbers, 0 to 255, separated by periods.)

Web - Click IP, General, Global Settings. Set IP Routing Status to Disabled to restrict operation to Layer 2, or Enabled to allow multilayer switching, specify the default gateway which will be forwarded packets for all unknown subnets, and click Apply.



CLI - This example enables IP routing, and sets the default gateway.

```
Console(config)#ip routing3-127
Console(config)#ip route default 10.1.0.2543-128
```


Downloaded from www.Manualslib.com manuals search engine

Configuring IP Routing Interfaces

You can specify the IP subnets connected to this router by manually assigning an IP address to each VLAN, or by using the RIP or OSPF dynamic routing protocol to identify routes that lead to other interfaces by exchanging protocol messages with other routers on the network.

Command Usage

- If this router is directly connected to end node devices (or connected to end nodes via shared media) that will be assigned to a specific subnet, then you must create a router interface for each VLAN that will support routing. The router interface consists of an IP address and subnet mask. This interface address defines both the network number to which the router interface is attached and the router's host number on that network. In other words, a router interface address defines the network and subnetwork numbers of the segment that is connected to that interface, and allows you to send IP packets to or from the router.

- Before you configure any network interfaces on this router, you should first create a VLAN for each unique user group, or for each network application and its associated users. Then assign the ports associated with each of these VLANs.

Command Attributes

- **VLAN ID** – ID of configured VLAN (1-4094, no leading zeroes).
- **IP Address Mode** – Specifies whether the IP address for this interface is statically assigned, or obtained from a network address server. (Options: Static, DHCP - Dynamic Host Configuration Protocol, BOOTP - Boot Protocol; Default: Static)
  - If Static address type is selected, then you must also specify whether the IP address is the primary IP address on the VLAN or a secondary IP address. An interface can have only one primary IP address, but can have multiple secondary IP addresses. In other words, you will need to specify secondary addresses if more than one IP subnet can accessed via this interface.

Downloaded from www.Manualslib.com manuals search engine

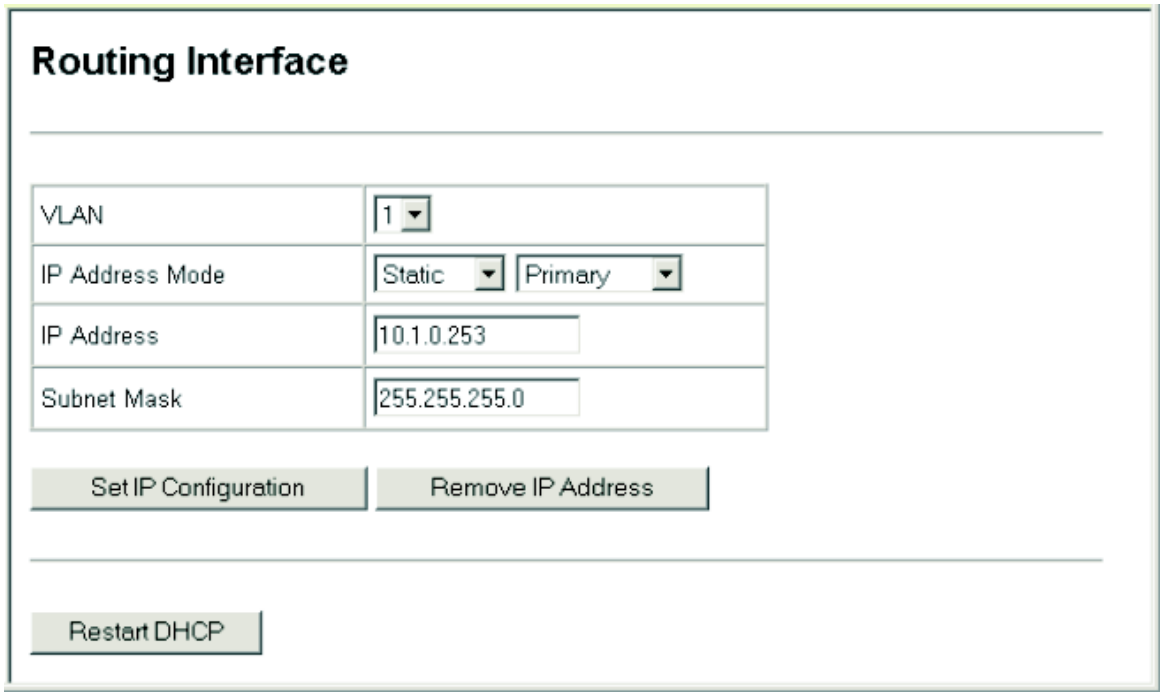
- If DHCP/BOOTP is enabled, IP will not function until a reply has been received from the address server. Requests will be broadcast periodically by the router for an IP address. (DHCP/ BOOTP values include the IP address and subnet mask.)

- **IP Address** – Address of the VLAN interface. Valid IP addresses consist of four numbers, 0 to 255, separated by periods.

- **Subnet Mask** – This mask identifies the host address bits used for routing to specific subnets.

Downloaded from www.Manualslib.com manuals search engine

Web - Click IP, General, Routing Interface. Specify an IP interface for each VLAN that will support routing to other subnets. First specify a primary address, and click Set IP Configuration. If you need to assign secondary addresses, enter these addresses one at a time, and click Set IP Configuration after entering each address.



CLI - This example sets a primary IP address for VLAN 1, and then adds a secondary IP address for a different subnet also attached to this router interface.

```
Console(config)#interface vlan 1
Console(config-if)#ip address 10.1.0.253 255.255.255.03-116
Console(config-if)#ip address 10.1.9.253 255.255.255.0 secondary
Console(config-if)#
```


Downloaded from www.Manualslib.com manuals search engine

Address Resolution Protocol

If IP routing is enabled (page 3-250), the router uses its routing tables to make routing decisions, and uses Address Resolution Protocol (ARP) to forward traffic from one hop to the next. ARP is used to map an IP address to a physical layer (i.e., MAC) address. When an IP frame is received by this router (or any standards- based router), it first looks up the MAC address corresponding to the destination IP address in the ARP cache. If the address is found, the router writes the MAC address into the appropriate field in the frame header, and forwards the frame on to the next hop. IP traffic passes along the path to its final destination in this way, with each routing device mapping the destination IP address to the MAC address of the next hop toward the recipient, until the packet is delivered to the final destination.

If there is no entry for an IP address in the ARP cache, the router will broadcast an ARP request packet to all devices on the network. The ARP request contains the following fields similar to that shown in this example:

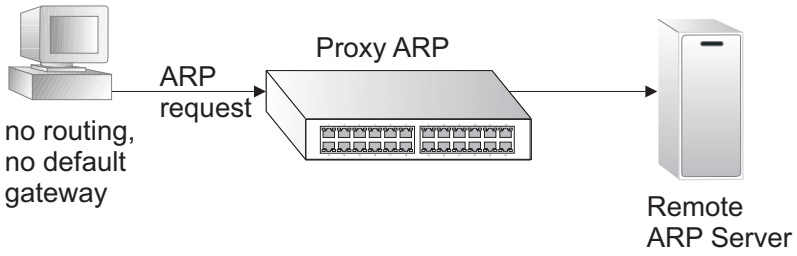
destination IP address	10.1.0.19
destination MAC address	?
source IP address	10.1.0.253
source MAC address	00-00-ab-cd-00-00

When devices receive this request, they discard it if their address does not match the destination IP address in the message. However, if it does match, they write their own hardware address into the destination MAC address field and send the message back to the source hardware address. When the source device receives a reply, it writes the destination IP address and corresponding MAC address into its cache, and forwards the IP traffic on to the next hop. As long as this entry has not timed out, the router will be able forward traffic directly to the next hop for this destination without having to broadcast another ARP request.

Downloaded from www.Manualslib.com manuals search engine

Proxy ARP

When a node in the attached subnetwork does not have routing or a default gateway configured, Proxy ARP can be used to forward ARP requests to a remote subnetwork. When the router receives an ARP request for a remote network and Proxy ARP is enabled, it determines if it has the best route to the remote network, and then answers the ARP request by sending its own MAC address to the requesting node. That node then sends traffic to the router, which in turn uses its own routing table to forward the traffic to the remote destination.



Basic ARP Configuration

You can use the ARP General configuration menu to specify the timeout for ARP cache entries, or to enable Proxy ARP for specific VLAN interfaces.

Command Usage

- The aging time determines how long dynamic entries remain the cache. If the timeout is too short, the router may tie up resources by repeating ARP requests for addresses recently flushed from the table.

- End stations that require Proxy ARP must view the entire network as a single network. These nodes must therefore use a smaller subnet mask than that used by the router or other relevant network devices.

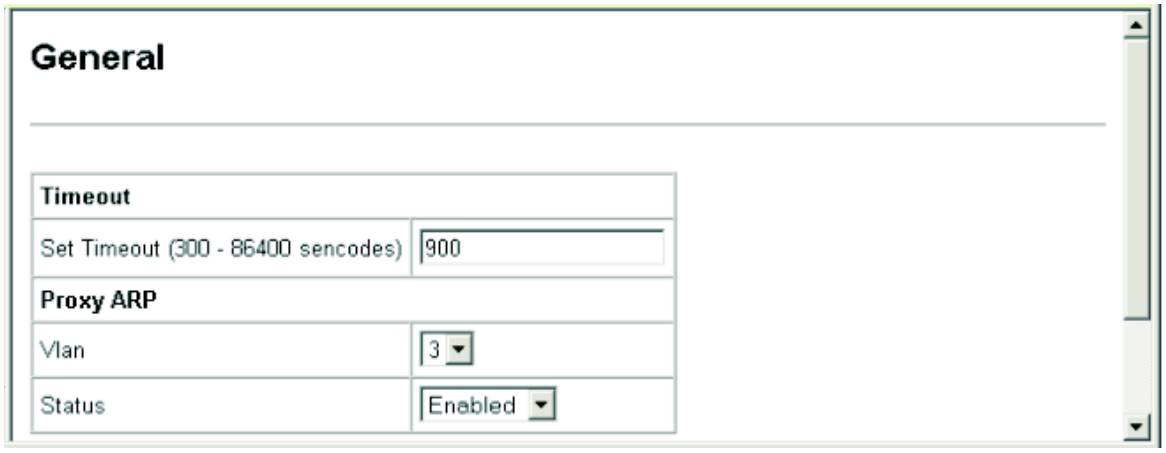
- Extensive use of Proxy ARP can degrade router performance because it may lead to increased ARP traffic and increased search time for larger ARP address tables.

Downloaded from www.Manualslib.com manuals search engine

Command Attributes

- **Timeout** – Sets the aging time for dynamic entries in the ARP cache. (Range: 300 - 86400 seconds; Default: 1200 seconds or 20 minutes)
- **Proxy ARP** – Enables or disables Proxy ARP for specified VLAN interfaces.

Web - Click IP, ARP, General. Set the timeout to a suitable value for the ARP cache, enable Proxy ARP for subnetworks that do not have routing or a default gateway, and click Apply.



CLI - This example sets the ARP cache timeout for 15 minutes (i.e., 900 seconds), and enables Proxy ARP for VLAN 3.

```
Console(config)#arp-timeout 900
Console(config)#interface vlan 3
Console(config-if)#ip proxy-arp
Console(config-if)#
```

Configuring Static ARP Addresses

For devices that do not respond to ARP requests, traffic will be dropped because the IP address cannot be mapped to a physical address. If this occurs, you can manually map an IP address to the corresponding physical address in the ARP.

Command Usage

- You can define up to 128 static entries in the ARP cache.
- Static entries will not be aged out or deleted when power is reset. You

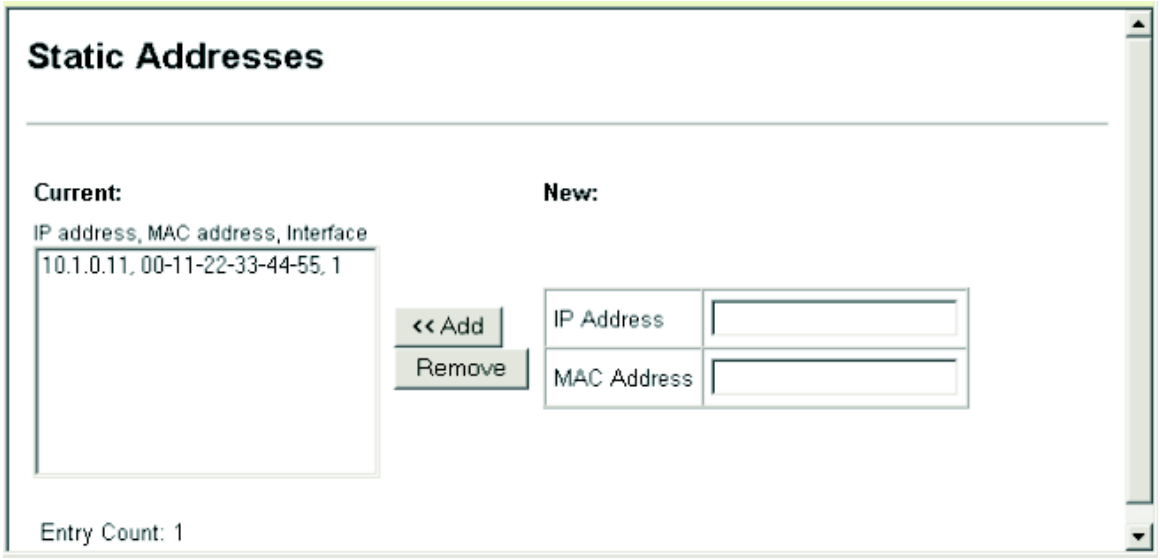
Downloaded from www.Manualslib.com manuals search engine

can only remove a static entry via the configuration interface.

Command Attributes

- **IP Address** – IP address statically mapped to a physical MAC address. (Valid IP addresses consist of four numbers, 0 to 255, separated by periods.)
- **MAC Address** – MAC address statically mapped to the corresponding IP address. (Valid MAC addresses are hexadecimal numbers in the format: xx-xx-xx-xx-xx-xx.)
- **Entry Count** – The number of static entries in the ARP cache.

Web - Click IP, ARP, Static Addresses. Enter the IP address, the corresponding MAC address, and click Apply.



CLI - This example sets a static entry for the ARP cache.

```
Console(config)#arp 10.1.0.11 00-11-22-33-44-553-122
Console(config)#
```

Displaying Dynamically Learned ARP Entries

The ARP cache contains entries that map IP addresses to the corresponding physical address. Most of these entries will be dynamically learned through replies to broadcast messages. You can display all of the dynamic entries in the ARP cache, change specific dynamic entries into static entries, or clear all dynamic entries from the cache.

Downloaded from www.Manualslib.com manuals search engine

Command Attributes

- **IP Address** – IP address of a dynamic entry in the cache.
- **MAC Address** – MAC address mapped to the corresponding IP address.
- **Interface** – VLAN interface associated with the address entry.
- **Dynamic to Static*** – Changes a selected dynamic entry to a static entry.
- **Clear All*** – Deletes all dynamic entries from the ARP cache.
- **Entry Count** – The number of dynamic entries in the ARP cache.

* These buttons take effect immediately. You are not prompted to confirm the action.

Web - Click IP, ARP, Dynamic Addresses. You can use the buttons provided to change a dynamic entry to a static entry, or to clear all dynamic entries in the cache.

Downloaded from www.Manualslib.com manuals search engine

CLI - This example shows all entries in the ARP cache.

```
Console#show arp3-124
Arp cache timeout: 1200 (seconds)

    IP Address       MAC Address      Type   Interface
--------------- ----------------- --------- -----------
       10.1.0.0 ff-ff-ff-ff-ff-ff     other           1
      10.1.0.11 00-11-22-33-44-55    static           1
      10.1.0.12 01-02-03-04-05-06    static           1
      10.1.0.19 00-10-b5-62-03-74   dynamic           1
     10.1.0.253 00-00-ab-cd-00-00     other           1
     10.1.0.255 ff-ff-ff-ff-ff-ff     other           1

Total entry : 6
Console#clear arp-cache3-124
This operation will delete all the dynamic entries in ARP Cache.
Are you sure to continue this operation (y/n)?y
Console#
```

Displaying Local ARP Entries

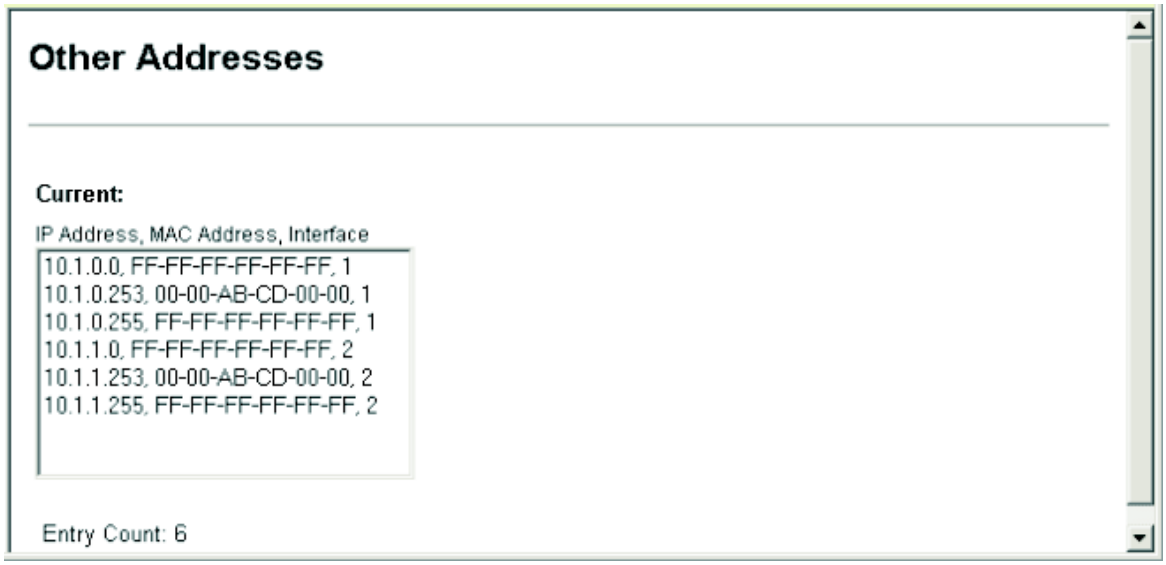
The ARP cache also contains entries for local interfaces, including subnet, host, and broadcast addresses.

Command Attributes

- **IP Address** – IP address of a local entry in the cache.
- **MAC Address** – MAC address mapped to the corresponding IP address.
- **Interface** – VLAN interface associated with the address entry.
- **Entry Count** – The number of local entries in the ARP cache.

Downloaded from www.Manualslib.com manuals search engine

Web - Click IP, ARP, Other Addresses.



CLI - This router uses the Type specification "other" to indicate local cache entries in the ARP cache.

```
Console#show arp3-124
Arp cache timeout: 1200 (seconds)

    IP Address       MAC Address      Type   Interface
--------------- ----------------- --------- -----------
       10.1.0.0 ff-ff-ff-ff-ff-ff     other           1
      10.1.0.11 00-11-22-33-44-55    static           1
      10.1.0.12 01-02-03-04-05-06    static           1
      10.1.0.19 00-10-b5-62-03-74   dynamic           1
     10.1.0.253 00-00-ab-cd-00-00     other           1
     10.1.0.255 ff-ff-ff-ff-ff-ff     other           1

Total entry : 6
Console#
```

Displaying ARP Statistics

You can display statistics for ARP messages crossing all interfaces on this router.

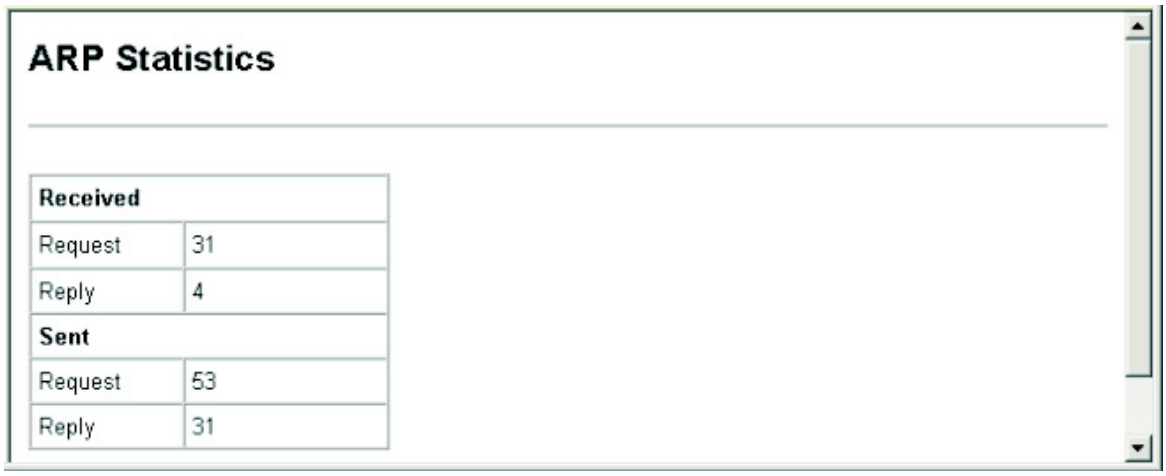
Statistical Values

Parameter	Description
Received Request	Number of ARP Request packets received by the router.
Received Reply	Number of ARP Reply packets received by the router.

Downloaded from www.Manualslib.com manuals search engine

Parameter	Description
Sent Request	Number of ARP Request packets sent by the router.
Sent Reply	Number of ARP Reply packets sent by the router.

Web - Click IP, ARP, Statistics.



CLI - This example provides detailed statistics on common IP-related protocols.

```
Console#show ip traffic3-130
IP statistics:
  Rcvd:  5 total, 5 local destination
         0 checksum errors
         0 unknown protocol, 0 not a gateway
  Frags: 0 reassembled, 0 timeouts
         0 fragmented, 0 couldn't fragment
  Sent:  9 generated
         0 no route
ICMP statistics:
  Rcvd: 0 checksum errors, 0 redirects, 0 unreachable, 0 echo
        5 echo reply, 0 mask requests, 0 mask replies, 0 quench
        0 parameter, 0 timestamp
  Sent: 0 redirects, 0 unreachable, 0 echo, 0 echo reply
        0 mask requests, 0 mask replies, 0 quench, 0 timestamp
        0 time exceeded, 0 parameter problem
UDP statistics:
  Rcvd: 0 total, 0 checksum errors, 0 no port
  Sent: 0 total
TCP statistics:
  Rcvd: 0 total, 0 checksum errors
  Sent: 0 total
ARP statistics:
  Rcvd: 0 requests, 1 replies
  Sent: 1 requests, 0 replies
```


Downloaded from www.Manualslib.com manuals search engine

Displaying Statistics for IP Protocols

IP Statistics

The Internet Protocol (IP) provides a mechanism for transmitting blocks of data (often called packets or frames) from a source to a destination, where these network devices (i.e., hosts) are identified by fixed length addresses. The Internet Protocol also provides for fragmentation and reassembly of long packets, if necessary, for transmission through "small packet" networks.

Statistical Values

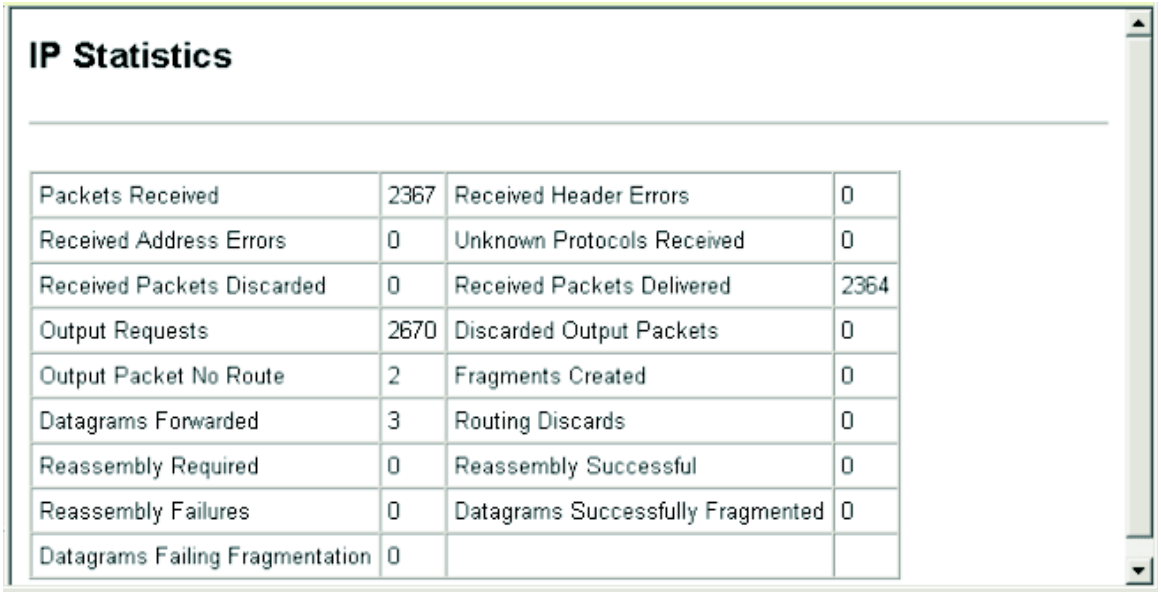
Parameter	Description
Packets Received	The total number of input datagrams received from interfaces, including those received in error.
Received Address Errors	The number of input datagrams discarded because the IP address in the header's destination field was not a valid address for this entity.
Received Packets Discarded	The number of input datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space).
Output Requests	The total number of datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission.
Output Packet No Route	The number of datagrams discarded because no route could be found to transmit them to their destination. Note that this includes any datagrams which a host cannot route because all of its default gateways are down.
Datagrams Forwarded	The number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination.
Reassembly Required	The number of IP fragments received which needed to be reassembled at this entity.
Reassembly Failures	The number of failures detected by the IP re-assembly algorithm (for whatever reason: timed out, errors, etc.).

Downloaded from www.Manualslib.com manuals search engine

Parameter	Description
Datagrams Failing Fragmentation	The number of datagrams that have been discarded because they needed to be fragmented at this entity but could not be, e.g., because their "Don't Fragment" flag was set.
Received Header Errors	The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, etc.
Unknown Protocols Received	The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
Received Packets Delivered	The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).
Discarded Output Packets	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space).
Fragments Created	The number of datagram fragments that have been generated as a result of fragmentation at this entity.
Routing Discards	The number of routing entries which were chosen to be discarded even though they are valid. One possible reason for discarding such an entry could be to free-up buffer space for other routing entries.
Reassembly Successful	The number of datagrams successfully re-assembled.
Datagrams Successfully Fragmented	The number of IP datagrams that have been successfully fragmented at this entity.

Downloaded from www.Manualslib.com manuals search engine

Web - Click IP, Statistics, IP.



IP Statistics

Packets Received	2367	Received Header Errors	0
Received Address Errors	0	Unknown Protocols Received	0
Received Packets Discarded	0	Received Packets Delivered	2364
Output Requests	2670	Discarded Output Packets	0
Output Packet No Route	2	Fragments Created	0
Datagrams Forwarded	3	Routing Discards	0
Reassembly Required	0	Reassembly Successful	0
Reassembly Failures	0	Datagrams Successfully Fragmented	0
Datagrams Failing Fragmentation	0		

CLI - See the example on page 3-261.

ICMP Statistics

Internet Control Message Protocol (ICMP) is a network layer protocol that transmits message packets to report errors in processing IP packets. ICMP is therefore an integral part of the Internet Protocol. ICMP messages may be used to report various situations, such as when a datagram cannot reach its destination, when the gateway does not have the buffering capacity to forward a datagram, and when the gateway can direct the host to send traffic on a shorter route. ICMP is also used by routers to feed back information about more suitable routes (i.e., the next hop router) to use for a specific destination.

Statistical Values

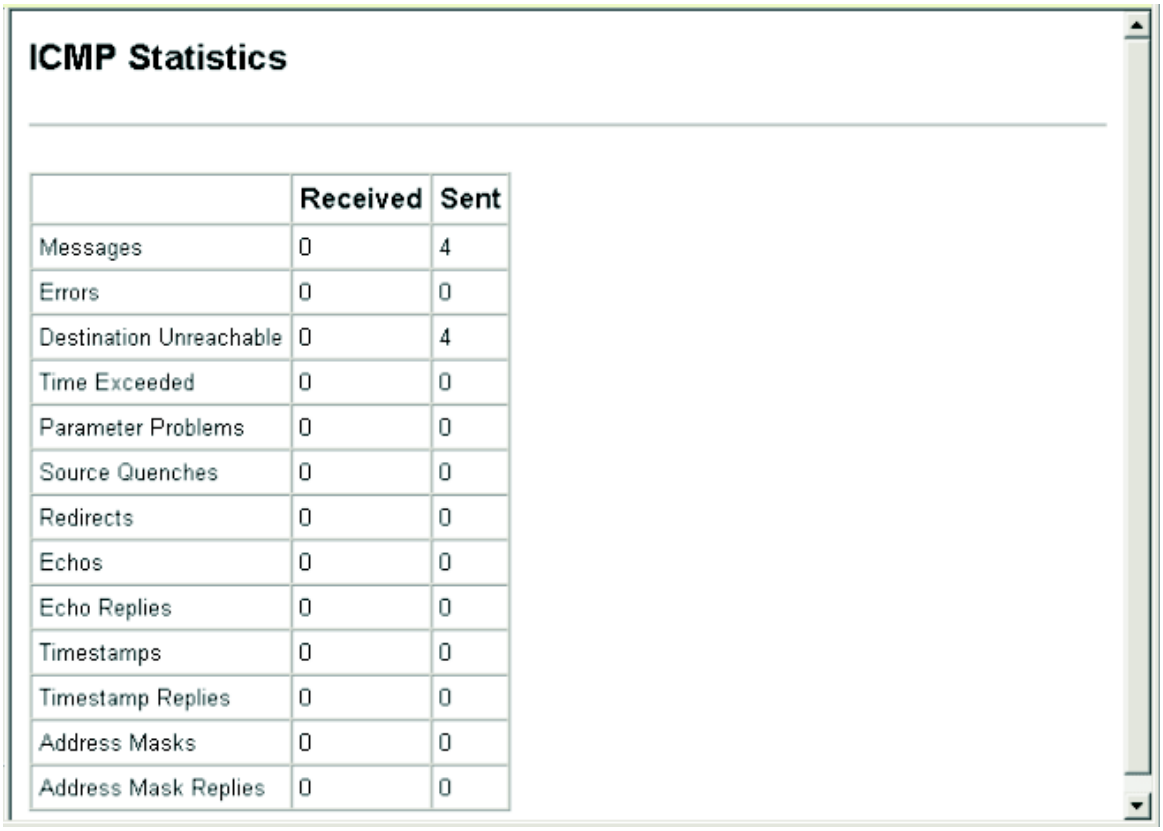
Parameter	Description
Messages	The total number of ICMP messages which the entity received/sent.
Errors	The number of ICMP messages which the entity received/sent but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.).

Downloaded from www.Manualslib.com manuals search engine

Parameter	Description
Destination Unreachable	The number of ICMP Destination Unreachable messages received/sent.
Time Exceeded	The number of ICMP Time Exceeded messages received/sent.
Parameter Problems	The number of ICMP Parameter Problem messages received/sent.
Source Quenches	The number of ICMP Source Quench messages received/sent.
Redirects	The number of ICMP Redirect messages received/sent.
Echos	The number of ICMP Echo (request) messages received/sent.
Echo Replies	The number of ICMP Echo Reply messages received/sent.
Timestamps	The number of ICMP Timestamp (request) messages received/sent.
Timestamp Replies	The number of ICMP Timestamp Reply messages received/sent.
Address Masks	The number of ICMP Address Mask Request messages received/sent.
Address Mask Replies	The number of ICMP Address Mask Reply messages received/sent.

Downloaded from www.Manualslib.com manuals search engine

Web - Click IP, Statistics, ICMP.



ICMP Statistics

	Received	Sent
Messages	0	4
Errors	0	0
Destination Unreachable	0	4
Time Exceeded	0	0
Parameter Problems	0	0
Source Quenches	0	0
Redirects	0	0
Echos	0	0
Echo Replies	0	0
Timestamps	0	0
Timestamp Replies	0	0
Address Masks	0	0
Address Mask Replies	0	0

CLI - See the example on page 3-261.

UDP Statistics

User Datagram Protocol (UDP) provides a datagram mode of packet-switched communications. It uses IP as the underlying transport mechanism, providing access to IP-like services. UDP packets are delivered just like IP packets – connection-less datagrams that may be discarded before reaching their targets. UDP is useful when TCP would be too complex, too slow, or just unnecessary.

Statistical Values

Parameter	Description
Datagrams Received	The total number of UDP datagrams delivered to UDP users.
Datagrams Sent	The total number of UDP datagrams sent from this entity.

Downloaded from www.Manualslib.com manuals search engine

Parameter	Description
Receive Errors	The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
No Ports	The total number of received UDP datagrams for which there was no application at the destination port.

Web - Click IP, Statistics, UDP.

CLI - See the example on page 3-261.

TCP Statistics

The Transmission Control Protocol (TCP) provides highly reliable host-to-host connections in packet-switched networks, and is used in conjunction with IP to support a wide variety of Internet protocols.

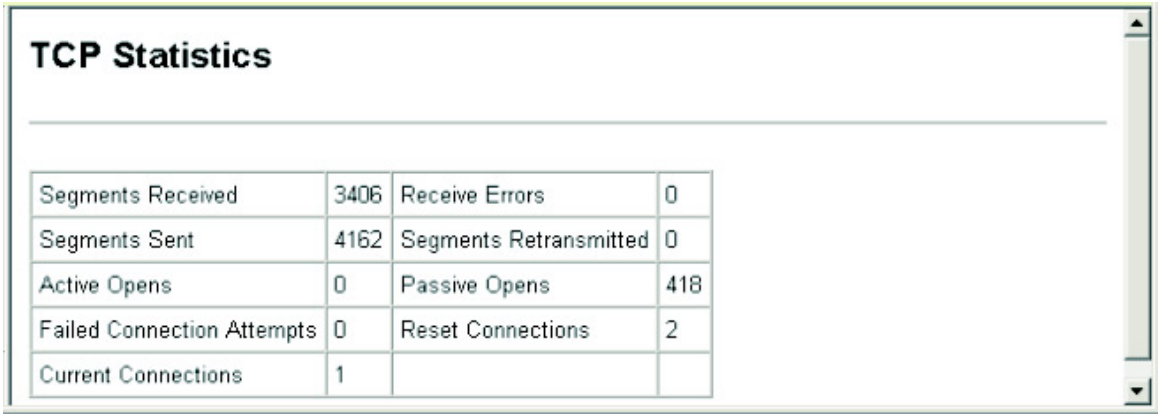
Statistical Values

Parameter	Description
Segments Received	The total number of segments received, including those received in error. This count includes segments received on currently established connections.
Segments Sent	The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.
Active Opens	The number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state.

Downloaded from www.Manualslib.com manuals search engine

Parameter	Description
Failed Connection Attempts	The number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state.
Current Connections	The number of TCP connections for which the current state is either ESTABLISHED or CLOSE- WAIT.
Receive Errors	The total number of segments received in error (e.g., bad TCP checksums).
Segments Retransmitted	The total number of segments retransmitted - that is, the number of TCP segments transmitted containing one or more previously transmitted octets.
Passive Opens	The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.
Reset Connections	The number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.

Web - Click IP, Statistics, TCP.


TCP Statistics
Segments Received 3406 Receive Errors 0
Segments Sent 4162 Segments Retransmitted 0
Active Opens 0 Passive Opens 418
Failed Connection Attempts 0 Reset Connections 2
Current Connections 1

CLI - See the example on page 3-261.

Configuring Static Routes

This router can dynamically configure routes to other network segments using dynamic routing protocols (i.e., RIP or OSPF). However, you can also manually enter static routes in the routing table. Static routes may be

Downloaded from www.Manualslib.com manuals search engine

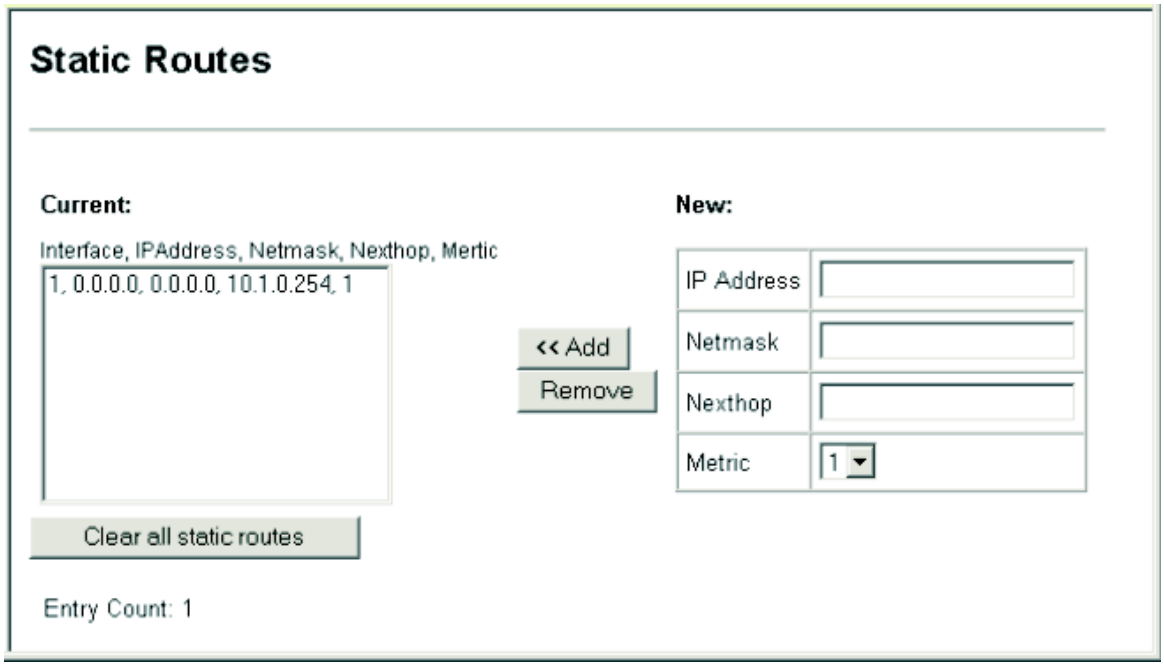
required to access network segments where dynamic routing is not supported, or can be set to force the use of a specific route to a subnet, rather than using dynamic routing. Static routes do not automatically change in response to changes in network topology, so you should only configure a small number of stable routes to ensure network accessibility.

Command Attributes

- **Interface** – Index number of the IP interface.
- **IP Address** – IP address of the destination network, subnetwork, or host.
- **Netmask** – Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.
- **Gateway** – IP address of the gateway used for this route.
- **Metric** – Cost for this interface. This cost is only used if a route is imported by a dynamic routing protocol such as OSPF. (Range: 1-5, default: 1)
- **Entry Count** – The number of table entries.

Downloaded from www.Manualslib.com manuals search engine

Web - Click IP, Routing, Static Routes.



CLI - This example forwards all traffic for subnet 192.168.1.0 to the router 192.168.5.254, using the default metric of 1.

```
Console(config)#ip route 192.168.1.0 255.255.255.0 192.168.5.254 3-128
Console(config)#
```

Displaying the Routing Table

You can display all the routes that can be accessed via the local network interfaces, via static routes, or via a dynamically learned route. If route information is available through more than one of these methods, the priority for route selection is local, static, and then dynamic. Also note that the route for a local interface is not enabled (i.e., listed in the routing table) unless there is at least one active link connected to that interface.

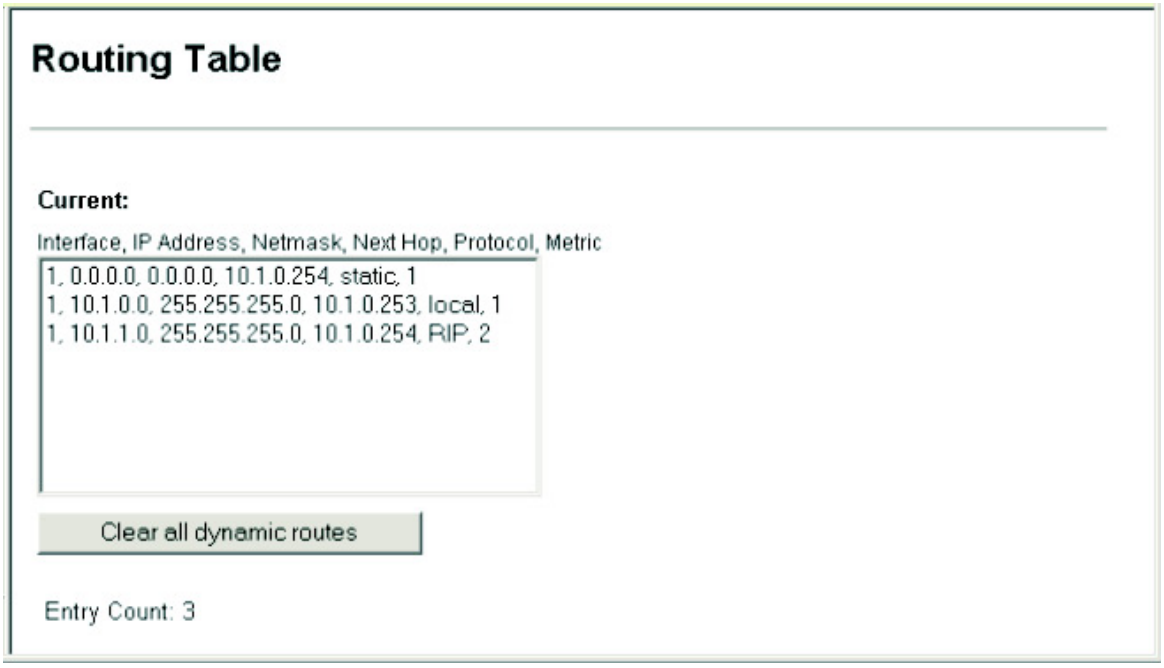
Command Attributes

- **Interface** – Index number of the IP interface.
- **IP Address** – IP address of the destination network, subnetwork, or host. Note that the address 0.0.0.0 indicates the default gateway for this router.

Downloaded from www.Manualslib.com manuals search engine

- **Netmask** – Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.
- **Next Hop** – The IP address of the next hop (or gateway) in this route.
- **Protocol** – The protocol which generated this route information. (Options: local, static, RIP, OSPF)
- **Metric** – Cost for this interface.
- **Entry Count** – The number of table entries.

Web - Click IP, Routing, Routing Table.


Routing Table
Current:
Interface, IP Address, Netmask, Next Hop, Protocol, Metric
1, 0.0.0.0, 0.0.0.0, 10.1.0.254, static, 1
1, 10.1.0.0, 255.255.255.0, 10.1.0.253, local, 1
1, 10.1.1.0, 255.255.255.0, 10.1.0.254, RIP, 2
Clear all dynamic routes
Entry Count: 3

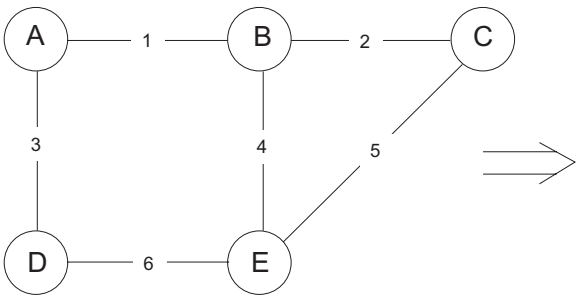
CLI - This example shows routes obtained from various methods.

```
Console#show ip route3-129

  Ip Address        Netmask        Next Hop     Protocol Metric Interface
--------------- --------------- --------------- -------- ------ ---------
        0.0.0.0         0.0.0.0      10.1.0.254   static      1         1
       10.1.0.0   255.255.255.0      10.1.0.253    local      1         1
       10.1.1.0   255.255.255.0      10.1.0.254      RIP      2         1

Total entries: 3
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Configuring the Routing Information Protocol

The RIP protocol is the most widely used routing protocol. The RIP protocol uses a distance-vector-based approach to routing. Routes are determined on the basis of minimizing the distance vector, or hop count, which serves as a rough estimate of transmission cost. Each router broadcasts its advertisement every 30 seconds, together with any updates to its routing table. This allows all routers on the network to learn consistent tables of next hop links which lead to relevant subnets.



Cost = 1 for all links

A	Link	Cost
A	0	0
B	1	1
C	1	2
D	3	1
E	1	2

Routing table for node A

Command Usage

- Just as Layer 2 switches use the Spanning Tree Algorithm to prevent loops, routers also use methods for preventing loops that would cause endless retransmission of data traffic. RIP utilizes the following three methods to prevent loops from occurring:

  - Split horizon – Never propagate routes back to an interface port from which they have been acquired.
  - Poison reverse – Propagate routes back to an interface port from which they have been acquired, but set the distance-vector metrics to infinity. (This provides faster convergence.)
  - Triggered updates – Whenever a route gets changed, broadcast an update message after waiting for a short random delay, but without waiting for the periodic cycle.

- RIP-2 is a compatible upgrade to RIP. RIP-2 adds useful capabilities for plain text authentication, multiple independent RIP domains, variable length subnet masks, and multicast transmissions for route advertising (RFC 1723).

Downloaded from www.Manualslib.com manuals search engine

- There are several serious problems with RIP that you should consider. First of all, RIP (version 1) has no knowledge of subnets, both RIP versions can take a long time to converge on a new route after the failure of a link or router during which time routing loops may occur, and its small hop count limitation of 15 restricts its use to smaller networks. Moreover, RIP (version 1) wastes valuable network bandwidth by propagating routing information via broadcasts; it also considers too few network variables to make the best routing decision.

Configuring General Protocol Settings

RIP is used to specify how routers exchange routing information. When RIP is enabled on this router, it sends RIP messages to all devices in the network every 30 seconds (by default), and updates its own routing table when RIP messages are received from other routers. To communicate properly with other routers using RIP, you need to specify the RIP version used globally by the router, as well as the RIP send and receive versions used on specific interfaces (page 3-277).

Command Usage

- When you specify a Global RIP Version, any VLAN interface not previously set to a specific Receive or Send Version (page 3-277) is set to the following values:
  - RIP Version 1 configures previously unset interfaces to send RIPv1 compatible protocol messages and receive either RIPv1 or RIPv2 protocol messages.
  - RIP Version 2 configures previously unset interfaces to use RIPv2 for both sending and receiving protocol messages.
- The *update* timer is the fundamental timer used to control all basic RIP processes.
  - Setting the update timer to a short interval can cause the router to spend an excessive amount of time processing updates. On the other hand, setting it to an excessively long time will make the routing protocol less sensitive to changes in the network configuration.

Downloaded from www.Manualslib.com manuals search engine

- The timers must be set to the same values for all routers in the network.

Command Attributes

Global Settings

- **RIP Routing Process** – Enables RIP routing for all IP interfaces on the router. (Default: Disabled)

- **Global RIP Version** – Specifies a RIP version used globally by the router. (Default: RIP Version 1)

Timer Settings

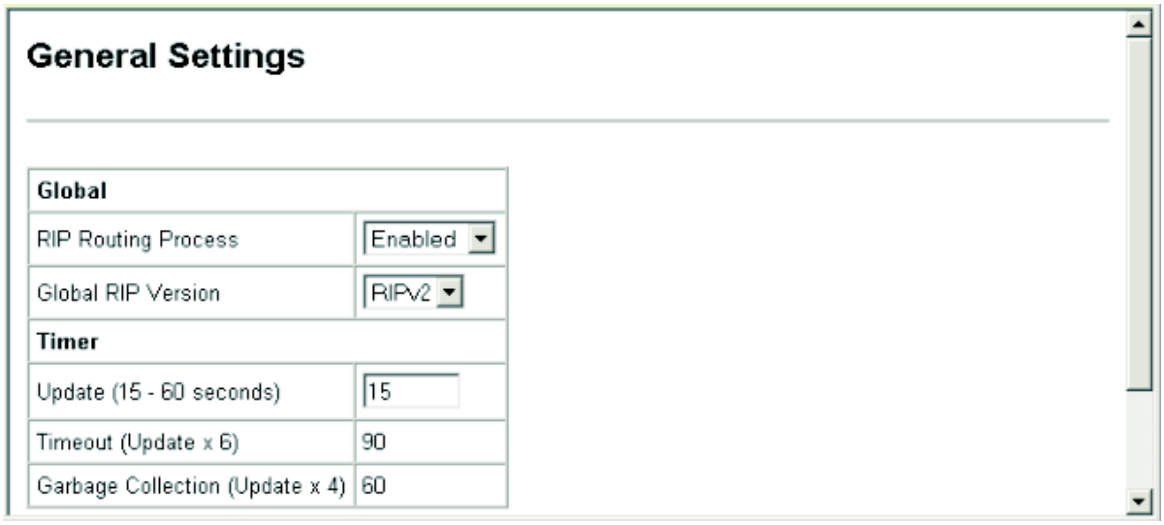
- **Update** – Sets the rate at which updates are sent. This value will also set the timeout timer to 6 times the update time, and the garbage-collection timer to 4 times the update time. (Range: 15-60 seconds; Default: 30 seconds)

- **Timeout** – Sets the time after which there have been no update messages that a route is declared dead. The route is marked inaccessible (i.e., the metric set to infinite) and advertised as unreachable. However, packets are still forwarded on this route. (Default: 180 seconds)

- **Garbage Collection** – After the *timeout* interval expires, the router waits for an interval specified by the *garbage-collection* timer before removing this entry from the routing table. This timer allows neighbors to become aware of an invalid route prior to purging. (Default: 120 seconds)

Downloaded from www.Manualslib.com manuals search engine

Web - Click Routing Protocol, RIP, General Settings. Enable or disable RIP, set the RIP version used on previously unset interfaces to RIPv1 or RIPv2, set the basic update timer, and then click Apply.



CLI - This example sets the router to use RIP Version 2, and sets the basic timer to 15 seconds.

```
Console(config)#router rip3-132
Console(config-router)#version 23-135
Console(config-router)#timers basic 153-133
Console(config-router)#end
Console#show rip globals3-142

RIP Process: Enabled
Update Time in Seconds: 15
Number of Route Change: 0
Number of Queries: 1
Console#
```

Specifying Network Interfaces for RIP

You must specify network interfaces that will be included in the RIP routing process.

Command Usage

- RIP only sends updates to interfaces specified by this command.
- Subnet addresses are interpreted as class A, B or C, based on the first field in the specified address. In other words, if a subnet address nnn.xxx.xxx.xxx is entered, the first field (nnn) determines the class:

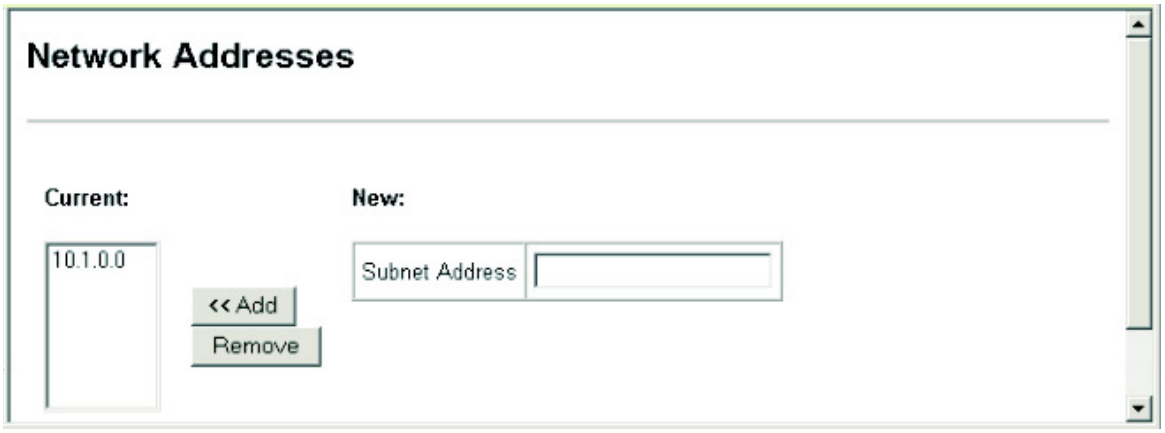
Downloaded from www.Manualslib.com manuals search engine

0 - 127 is class A, and only the first field in the network address is used.
128 - 19 is class B, and the first two fields in the network address are used.
192 - 223 is class C, and the first three fields in the network address are used.

Command Attributes

- **Subnet Address** – IP address of a network directly connected to this router.

Web - Click Routing Protocol, RIP, Network Addresses. Add all interfaces that will participate in RIP, and click Apply.



CLI - This example includes network interface 10.1.0.0 in the RIP routing process.

```
Console(config)#router-rip3-132
Console(config-router)#network 10.1.0.03-134
Console(config-router)#end
Console#show ip rip status3-143

          Peer   UpdateTime   Version   RcvBadPackets   RcvBadRoutes
--------------- ------------ --------- --------------- --------------
     10.1.0.253              0               0               73
     10.1.1.253              0               0               66

Console#
```

Configuring Network Interfaces for RIP

For each interface that participates in the RIP routing process, you must specify the protocol message type accepted (i.e., RIP version) and the

Downloaded from www.Manualslib.com manuals search engine

message type sent (i.e., RIP version or compatibility mode), the method for preventing loopback of protocol messages, and whether or not authentication is used (i.e., authentication only applies if RIPv2 messages are being sent or received).

Command Usage

Specifying Receive and Send Protocol Types

- Setting the RIP Receive Version or Send Version for an interface overrides the global setting specified by the RIP / General Settings, Global RIP Version field.

- You can specify the Receive Version based on these options:
  - Use "RIPv1" or "RIPv2" if all routers in the local network are based on RIPv1 or RIPv2, respectively.
  - Use "RIPv1 or RIPv2" if some routers in the local network are using RIPv2, but there are still some older routers using RIPv1.
  - Use "Do Not Receive" if you do not want to add any dynamic entries to the routing table for an interface. (For example, you may only want to allow static routes for a specific interface.)
- You can specify the Send Version based on these options:
  - Use "RIPv1" or "RIPv2" if all routers in the local network are based on RIPv1 or RIPv2, respectively.
  - Use "RIPv1 Compatible" to propagate route information by broadcasting to other routers on the network using the RIPv2 advertisement list, instead of multicasting as normally required by RIPv2. (Using this mode allows RIPv1 routers to receive these protocol messages, but still allows RIPv2 routers to receive the additional information provided by RIPv2, including subnet mask, next hop and authentication information.)
  - Use "Do Not Send" to passively monitor route information advertised by other routers attached to the network.

Loopback Prevention

Just as Layer 2 switches use the Spanning Tree Algorithm to prevent loops, routers also use methods for preventing loops that would cause endless

Downloaded from www.Manualslib.com manuals search engine

retransmission of data traffic. When protocol packets are caught in a loop, links will be congested, and protocol packets may be lost. However, the network will slowly converge to the new state. RIP utilizes the following three methods that can provide faster convergence when the network topology changes and prevent most loops from occurring:

- Split Horizon – Never propagate routes back to an interface port from which they have been acquired.
- Poison Reverse – Propagate routes back to an interface port from which they have been acquired, but set the distance-vector metrics to infinity. (This provides faster convergence.)
- Triggered Updates – Whenever a route gets changed, broadcast an update message after waiting for a short random delay, but without waiting for the periodic cycle.

Protocol Message Authentication

RIPv1 is not a secure protocol. Any device sending protocol messages from UDP port 520 will be considered a router by its neighbors. Malicious or unwanted protocol messages can be easily propagated throughout the network if no authentication is required. RIPv2 supports authentication via a simple password. When a router is configured to exchange authentication messages, it will insert the password into all transmitted protocol packets, and check all received packets to ensure that they contain the authorized password. If any incoming protocol messages do not contain the correct password, they are simply dropped.

Command Attributes

- **VLAN** – ID of configured VLAN (1-4094).

- **Receive Version** – The RIP version to receive on an interface.
  - **RIPv1**: Accepts only RIPv1 packets.
  - **RIPv2**: Accepts only RIPv2 packets.
  - **RIPv1 or RIPv2**: Accepts RIPv1 or RIPv2 packets. (Default)
  - **Do Not Receive**: Does not accept incoming RIP packets.

(The default depends on the setting specified under RIP / General Settings, Global RIP Version: RIPv1 - RIPv1 or RIPv2 packets, RIPv2 - RIPv2 packets)

Downloaded from www.Manualslib.com manuals search engine

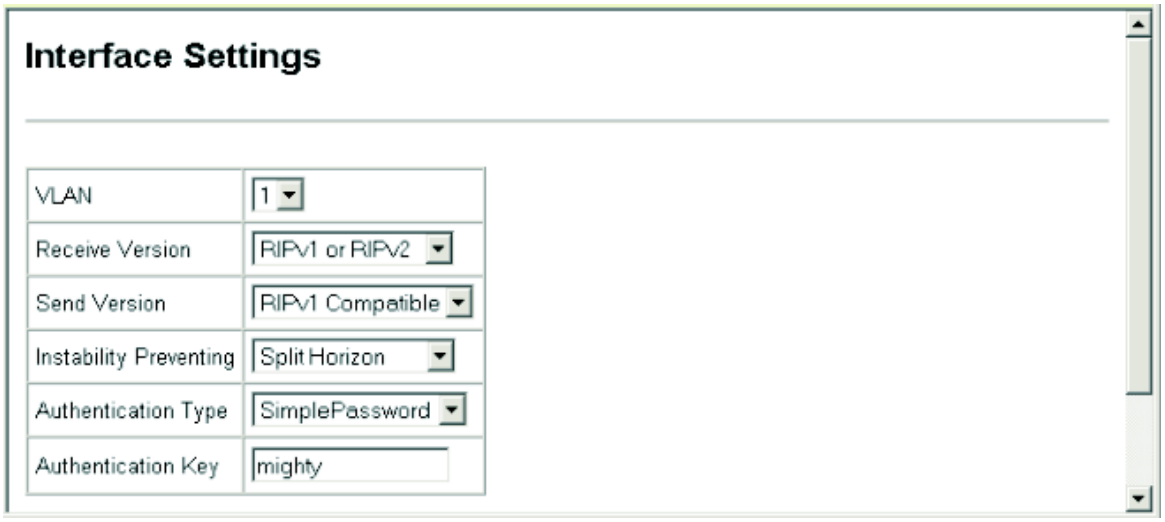
- **Send Version** – The RIP version to send on an interface.
  - **RIPv1**: Sends only RIPv1 packets.
  - **RIPv2**: Sends only RIPv2 packets.
  - **RIPv1 Compatible**: Route information is broadcast to other routers with RIPv2. (Default)
  - **Do Not Send**: Does not transmit RIP updates.

(The default depends on the setting specified under RIP / General Settings, Global RIP Version: RIPv1 - RIPv1 Compatible, RIPv2 - RIPv2 packets)

- **Instability Preventing** – Specifies the method used to reduce the convergence time when the network topology changes, and to prevent RIP protocol messages from looping back to the source router. (Default: Split Horizon)
  - **None**: No method is used. If a loop occurs, the hop count for a route may be gradually incremented to infinity (i.e., 16) before the route is deemed unreachable.
  - **Split Horizon**: This method never propagates routes back to an interface from which they have been acquired.
  - **Poision Reverse**: This method propagates routes back to an interface port from which they have been acquired, but set the distance-vector metrics to infinity. (This provides faster convergence.)
- **Authentication Type** – Specifies whether or not authentication is required for exchanging protocol messages. (Default: No Authentication)
  - **No Authentication**: No authentication is required.
  - **Simple Password**: Requires the interface to exchange routing information with other routers based on an authorized password. (Note that authentication only applies to RIPv2.)
- **Authentication Key** – Specifies the key to use for authenticating RIPv2 packets. For authentication to function properly, both the sending and receiving interface must use the same password. (Range: 1-16 characters, case sensitive)

Downloaded from www.Manualslib.com manuals search engine

Web - Click Routing Protocol, RIP, Interface Settings. Select the RIP protocol message types that will be received and sent, the method used to provide faster convergence and prevent loopback (i.e., prevent instability in the network topology), and the authentication option and corresponding password. Then click Apply.



CLI - This example sets the receive version to accept both RIPv1 or RIPv2 messages, the send mode to RIPv1 compatible (i.e., called v2-broadcast in the CLI), sets the method of preventing instability in the network topology to Split Horizon, enables authentication via a simple password (i.e., called text mode in the CLI).

```
Console(config)#interface vlan 1 3-1
Console(config-if)#ip rip receive version 1 2 3-137
Console(config-if)#ip rip send version v2-broadcast 3-138
Console(config-if)#ip split-horizon 3-139
Console(config-if)#ip rip authentication mode text 3-141
Console(config-if)#ip rip authentication key mighty 3-140
Console#
```

Displaying RIP Information and Statistics

You can display basic information about the current global configuration settings for RIP, statistics about route changes and queries, information about the interfaces on this router that are using RIP, and information about known RIP peer devices.

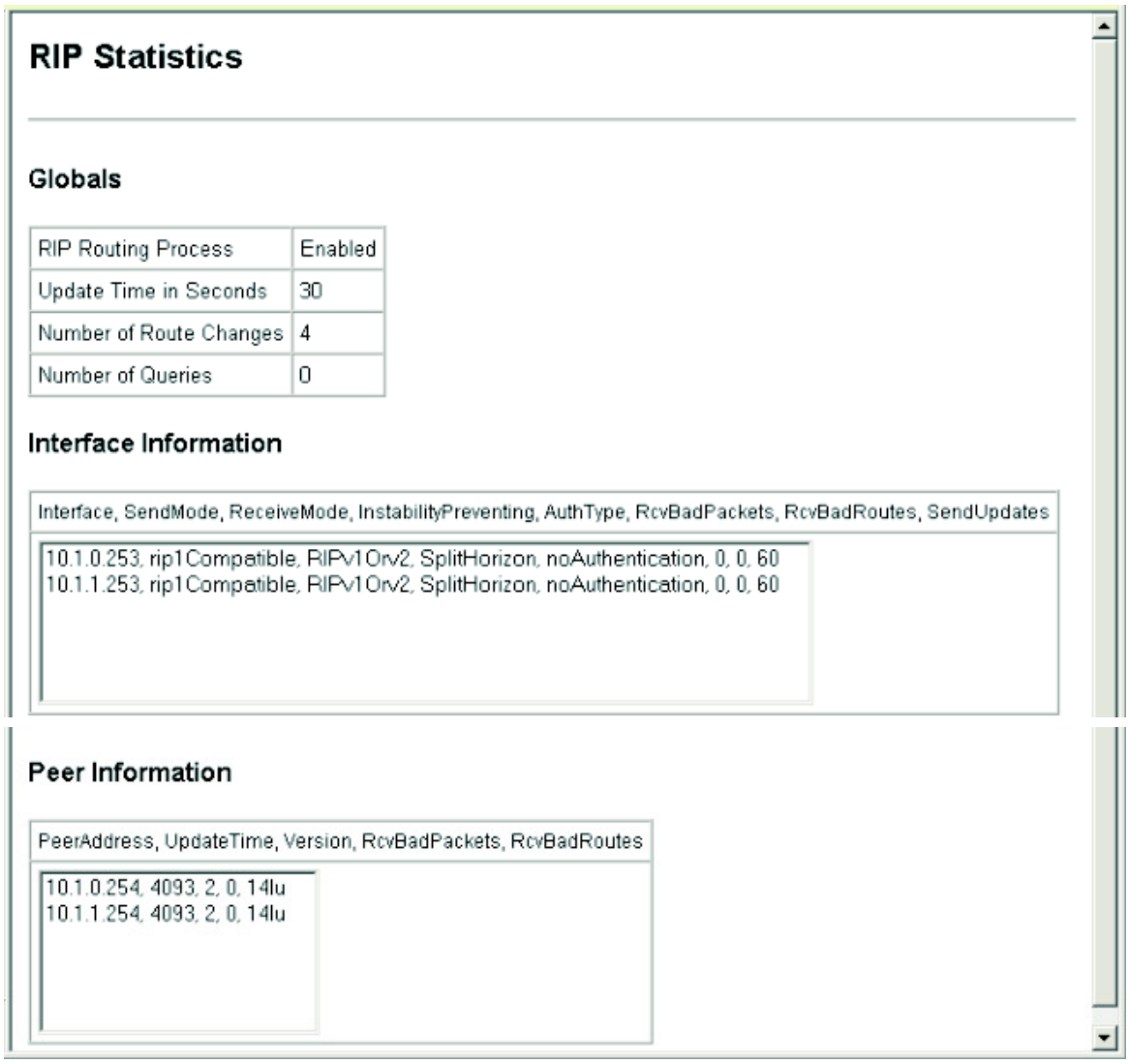
Downloaded from www.Manualslib.com manuals search engine

RIP Information and Statistics

Parameter	Description
Globals	
RIP Routing Process	Indicates if RIP has been enabled or disabled.
Update Time in Seconds	The interval at which RIP advertises known route information. (Default: 30 seconds)
Number of Route Changes	Number of times routing information has changed.
Number of Queries	Number of router database queries received by this router.
Interface Information	
Interface	IP address of the interface.
SendMode	RIP version sent on this interface (none, RIPv1, RIPv2, rip1Compatible).
ReceiveMode	RIP version received on this interface (none, RIPv1, RIPv2, RIPv1Orv2).
InstabilityPreventing	Shows if split-horizon, poison-reverse, or no instability prevention method is in use.
AuthType	Shows if authentication is set to simple password or none.
RcvBadPackets	Number of bad RIP packets received.
RcvBadRoutes	Number of bad routes received.
SendUpdates	Number of route changes.
Peer Information	
PeerAddress	IP address of a neighboring RIP router.
UpdateTime	Last time a route update was received from this peer.
Version	Whether RIPv1 or RIPv2 packets were received from this peer.
RcvBadPackets	Number of bad RIP packets received from this peer.
RcvBadRoutes	Number of bad routes received from this peer.

Downloaded from www.Manualslib.com manuals search engine

Web - Click Routing Protocol, RIP, Statistics.



RIP Statistics

Globals

RIP Routing Process	Enabled
Update Time in Seconds	30
Number of Route Changes	4
Number of Queries	0

Interface Information

Interface, SendMode, ReceiveMode, InstabilityPreventing, AuthType, RcvBadPackets, RcvBadRoutes, SendUpdates
10.1.0.253, rip1Compatible, RIPv1Orv2, SplitHorizon, noAuthentication, 0, 0, 60 10.1.1.253, rip1Compatible, RIPv1Orv2, SplitHorizon, noAuthentication, 0, 0, 60

Peer Information

PeerAddress, UpdateTime, Version, RcvBadPackets, RcvBadRoutes
10.1.0.254, 4093, 2, 0, 14lu 10.1.1.254, 4093, 2, 0, 14lu

Downloaded from www.Manualslib.com manuals search engine

CLI - The information displayed by the RIP Statistics screen via the web interface can be accessed from the CLI using the following commands.

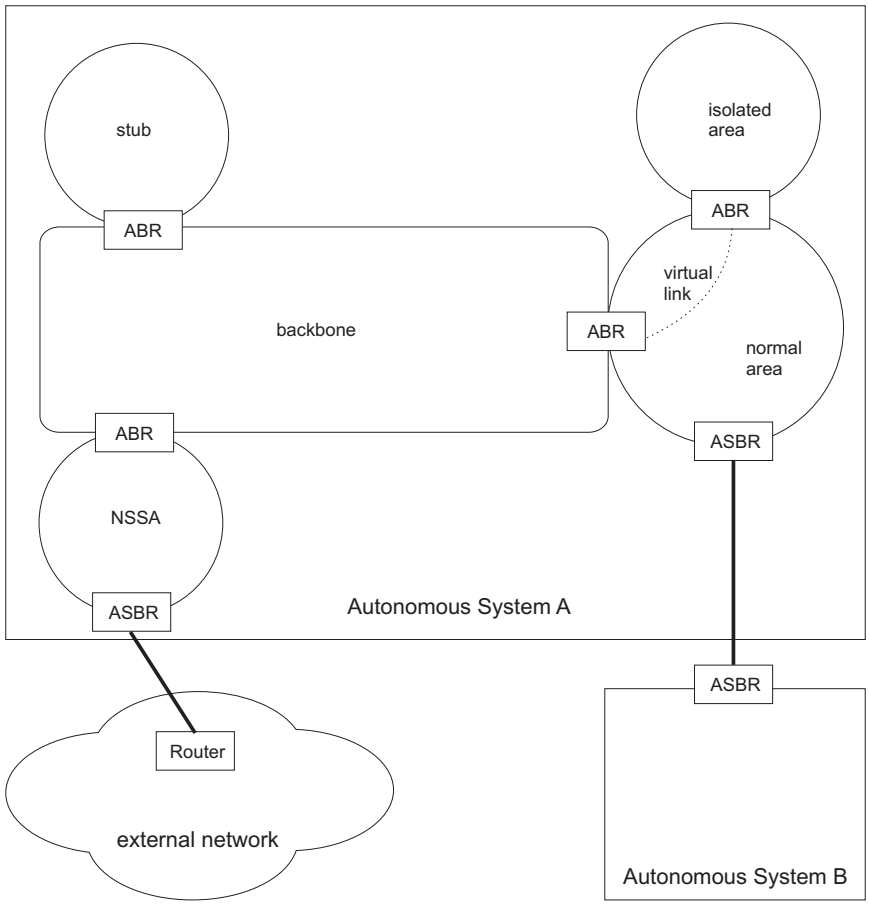
```
Console#show rip globals3-142

RIP Process: Enabled
Update Time in Seconds: 30
Number of Route Change: 4
Number of Queries: 0
Console#show ip rip configuration3-143

     Interface      SendMode      ReceiveMode     Poison       Authentication
--------------- --------------- ------------- --------------
------------------
     10.1.0.253  rip1Compatible     RIPv1Orv2   SplitHorizon
noAuthentication
     10.1.1.253  rip1Compatible     RIPv1Orv2   SplitHorizon
noAuthentication
Console#show ip rip status3-143

     Interface   RcvBadPackets   RcvBadRoutes     SendUpdates
--------------- --------------- -------------- ---------------
     10.1.0.253               0              0              60
     10.1.1.253               0              0              63
Console#show ip rip peer3-143

          Peer   UpdateTime   Version   RcvBadPackets   RcvBadRoutes
--------------- ------------ --------- --------------- --------------
     10.1.0.254         4610         2               0              0
     10.1.1.254         4610         2               0              0
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Configuring the Open Shortest Path First Protocol

Open Shortest Path First (OSPF) is more suited for large area networks which experience frequent changes in the links. It also handles subnets much better than RIP. OSPF protocol actively tests the status of each link to its neighbors to generate a shortest path tree, and builds a routing table based on this information. OSPF then utilizes IP multicast to propagate routing information. A separate routing area scheme is also used to further reduce the amount of routing traffic.

Note: The OSPF protocol implemented in this device is based on Version 2 (RFC 2328). It also supports Version 1 (RFC 1583) compatibility mode to ensure that the same method is used to calculate summary route costs throughout the network when older OSPF routers exist; as well as the not-so-stubby area option (RFC 1587).



Downloaded from www.Manualslib.com manuals search engine

Command Usage

- OSPF looks at more than just the simple hop count. When adding the shortest path to any node into the tree, the optimal path is chosen on the basis of delay, throughput and connectivity. OSPF utilizes IP multicast to reduce the amount of routing traffic required when sending or receiving routing path updates. The separate routing area scheme used by OSPF further reduces the amount of routing traffic, and thus inherently provides another level of routing protection. In addition, all routing protocol exchanges can be authenticated. Finally, the OSPF algorithms have been tailored for efficient operation in TCP/IP Internets.

- OSPFv2 is a compatible upgrade to OSPF. It involves enhancements to protocol message authentication, and the addition of a point-to-multipoint interface which allows OSPF to run over non-broadcast networks, as well as support for overlapping area ranges.

- When using OSPF, you must organize your network (i.e., autonomous system) into normal, stub, or not-so-stubby areas; configure the ranges of subnet addresses that can be aggregated by link state advertisements; and configure virtual links for areas that do not have direct physical access to the OSFP backbone.

    - To implement OSPF for a large network, you must first organize the network into logical areas to limit the number of OSPF routers that actively exchange Link State Advertisements (LSAs). You can then define an OSPF interface by assigning an IP interface configured on this router to one of these areas. This OSPF interface will send and receive OSPF traffic to neighboring OSPF routers.
    - You can further optimize the exchange of OSPF traffic by specifying an area range that covers a large number of subnetwork addresses. This is an important technique for limiting the amount of traffic exchanged between Area Border Routers (ABRs).

Downloaded from www.Manualslib.com manuals search engine

- And finally, you must specify a virtual link to any OSPF area that is not physically attached to the OSPF backbone. Virtual links can also be used to provide a redundant link between contiguous areas to prevent areas from being partitioned, or to merge backbone areas.

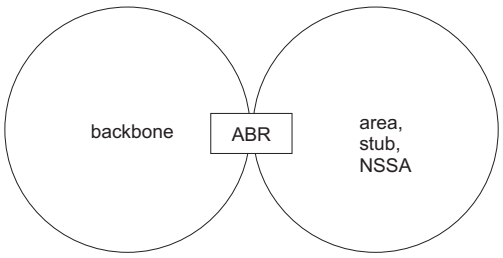
Configuring General Protocol Settings

To implement dynamic OSPF routing, first assign VLAN groups to each IP subnet to which this router will be attached, then use the OSPF / General Configuration menu to enable OSPF, assign an Router ID to this device, and set the other basic protocol parameters.

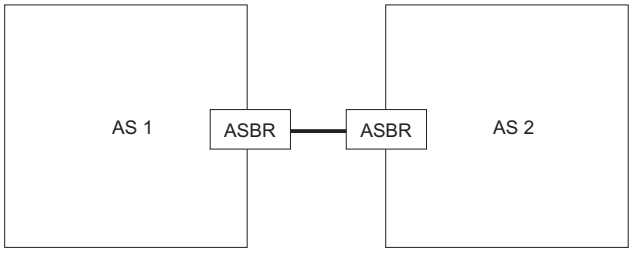
Command Attributes

General Information –

- **OSPF Routing Process** – Enables or disables OSPF routing for all IP interfaces on the router. (Default: Disabled)
- **OSPF Router ID** – Assigns a unique router ID for this device within the autonomous system. (Default: The lowest interface address)
- **Version Number** [1] – This router only supports OSPF Version 2.
- **Area Border Router** [1] – Indicates if this router connect directly to networks in two or more areas. An area border router runs a separate copy of the Shortest Path First algorithm, maintaining a separate routing database for each area.



- **AS Boundary Router** [2] – Allows this router to exchange routing information with boundary routers in other autonomous



Downloaded from www.Manualslib.com manuals search engine

systems to which it may be attached. If a router is enabled as an ASBR, then every other router in the autonomous system can learn about external routes from this device. (Default: Disabled)

- **Rfc1583 Compatible** – If one or more routers in a routing domain are using OSPF Version 1, this router should use RFC 1583 (OSPFv1) compatibility mode to ensure that all routers are using the same RFC for calculating summary route costs. Enable this field to force the router to calculate summary route costs using RFC 1583. (Default: Disabled)

- **Auto Cost (Mbps)** [1] – This is the reference bandwidth used to calculate the default cost metric for each interface. To change the cost metric for any interface, use the OSP / Interface Configuration screen. (Default: 100)
- **SPF Hold Time (seconds)** – The hold time between making two consecutive shortest path first (SPF) calculations. (Range: 0-65535; Default: 10)

- **Area Numbers** [1] – The number of OSPF areas configured on this router.

Default Route Information –

- **Originate Default Route** [2] – Generates a default external route into an autonomous system. Note that the **AS Boundary Router** field must be enabled, and the **Advertise Default Route** field properly configured. (Default: Disabled)
- **Advertise Default Route** [2] – The router can advertise a default external route into the autonomous system (AS). (Options: NotAlways, Always; Default: NotAlways)
  - **Always** – The router will advertise itself as a default external route for the AS, even if a default external route does not actually exist.
  - **NotAlways** – It can only advertise a default external route into the AS if it has been configured to import external routes via RIP

Downloaded from www.Manualslib.com manuals search engine

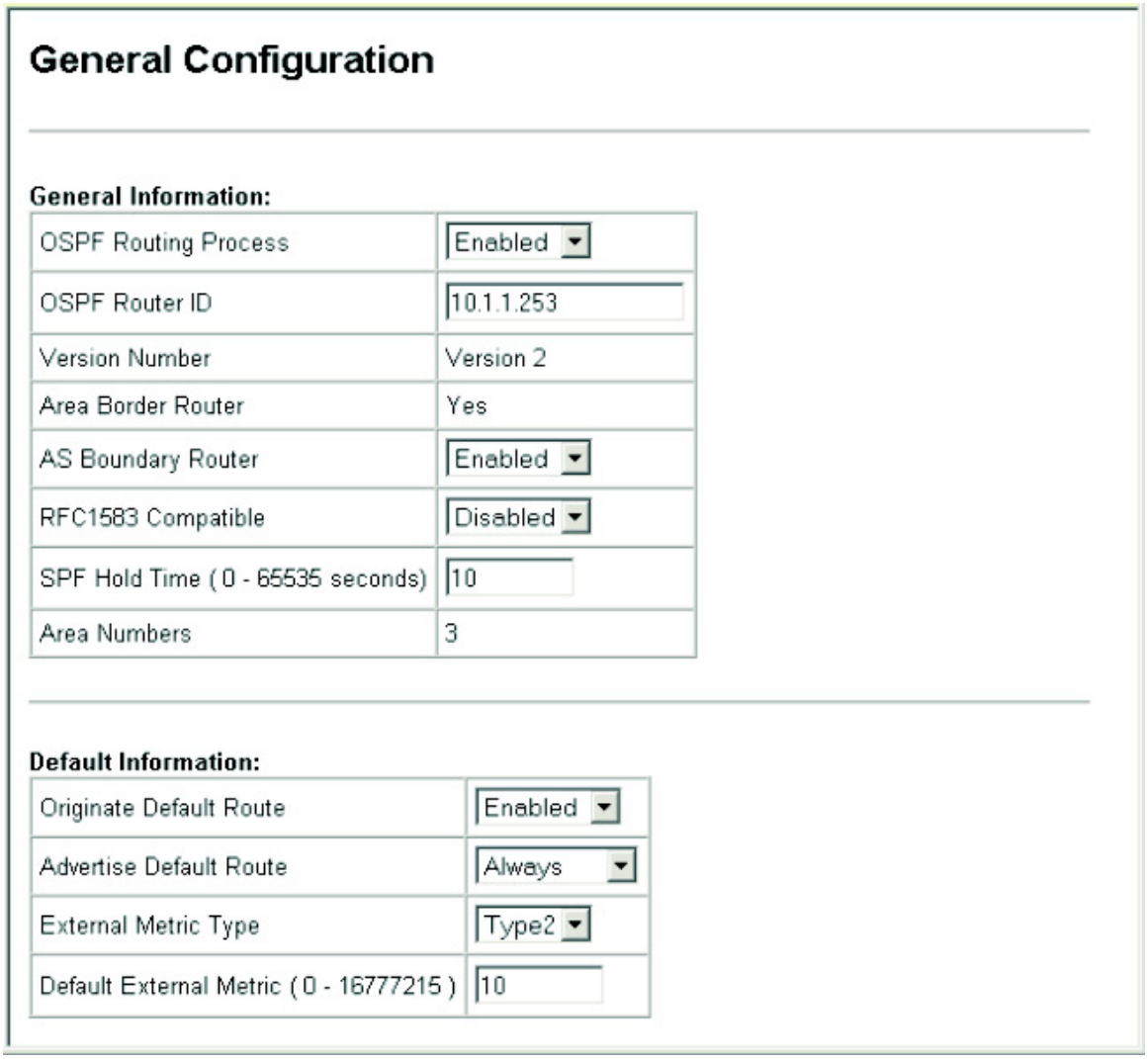
or static configuration, and such a route is known. (See "Redistributing External Routes" on page 3-310.)

- **External Metric Type** [2] – The external link type used to advertise the default route. Type 1 route advertisements add the internal cost to the external route metric. Type 2 routes do not add the internal cost metric. When comparing Type 2 routes, the internal cost is only used as a tie-breaker if several Type 2 routes have the same cost. (Default: Type 2)
- **Default External Metric** [2] – The Metric assigned to the default route. (Range: 1-65535; Default: 10)

1. These items are read only.
2. CLI - These items are configured with the **default-information originate** command (page 3-149).

Downloaded from www.Manualslib.com manuals search engine

Web - Click Routing Protocol, OSPF, General Configuration. Enable OSPF, specify the Router ID, configure the other global parameters as required, and click Apply.



CLI - This example configures the router with the same settings as shown in the screen capture for the web interface.

```
Console(config)#router ospf3-146
Console(config-router)#router-id 10.1.1.2533-147
Console(config-router)#no compatible rfc15833-148
Console(config-router)#default-information originate always
metric 10 metric-type 23-149
Console(config-router)#timers spf 103-150
Console(config-router)#
```

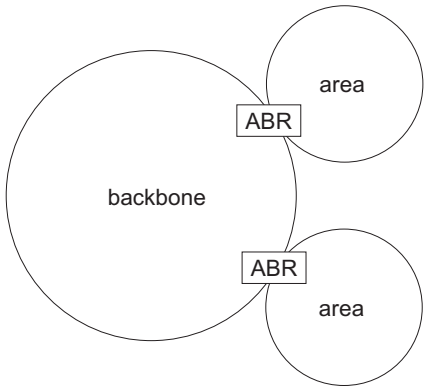

Downloaded from www.Manualslib.com manuals search engine

Configuring OSPF Areas

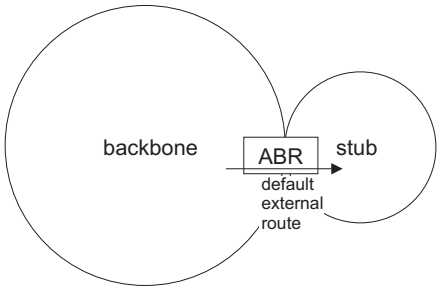
An autonomous system must be configured with a backbone area, designated by area identifier 0.0.0.0. By default, all other areas are created as normal transit areas.

Routers in a normal area may import or export routing information about individual nodes. To reduce the amount of routing traffic flooded onto the network, you can configure an area to export a single summarized route that covers a broad range of network addresses within the area (page 3-295). To further reduce the amount of routes passed between areas, you can configure an area as a stub or a not-so-stubby area (NSSA).

Normal Area – A large OSPF domain should be broken up into several areas to increase network stability and reduce the amount of routing traffic required through the use of route summaries that aggregate a range of addresses into a single route. The backbone or any normal area can pass traffic between other areas, and are therefore known as transit areas. Each router in an area has identical routing tables. These tables may include area links, summarized links, or external links that depict the topology of the autonomous system.



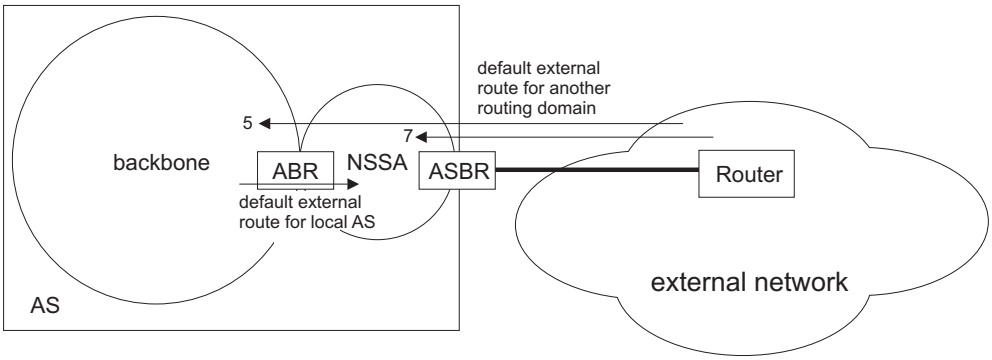
Stub – A stub does not accept external routing information. Instead, an area border router adjacent to a stub can be configured to send a default external route into the stub for all destinations outside the local area or the autonomous system. This route will also be advertised as a single entry point for traffic entering the stub. Using a stub can significantly reduce the amount of topology data that has to be exchanged over the network.



Downloaded from www.Manualslib.com manuals search engine

- By default, a stub can only pass traffic to other areas in the autonomous system via the default external route. However, you also can configure an area border router to send Type 3 summary link advertisements into the stub.

NSSA – A not-so-stubby area (NSSA) is similar to a stub. It blocks most external routing information, and can be configured to advertise a single default route for traffic passing between the NSSA and other areas within the autonomous system (AS). However, an NSSA can also import external routes from one or more small routing domains that are not part of the AS, such as a RIP domain or locally configured static routes. This external AS routing information is generated by the NSSA's ASBR and advertised only within the NSSA. By default, these routes are not flooded onto the backbone or into any other area by area border routers. However, the NSSA's ABRs will convert NSSA external LSAs (Type 7) into external LSAs (Type-5) which are propagated into other areas within the AS.



- Routes that can be advertised with NSSA external LSAs include network destinations outside the AS learned via OSPF, the default route, static routes, routes derived from other routing protocols such as RIP, or directly connected networks that are not running OSPF.
- Also, note that unlike stub areas, all Type-3 summary LSAs are always imported into NSSAs to ensure that internal routes are always chosen over Type-7 NSSA external routes.

Default Cost – This specifies a cost for the default summary route sent into a stub or not-so-stubby area (NSSA) from an Area Border Router (ABR).

Downloaded from www.Manualslib.com manuals search engine

Command Usage

- Before you create a stub or NSSA, first specify the address range for an area using the Network Area Address Configuration screen (page 3-305).
- Stubs and NSSAs cannot be used as a transit area, and should therefore be placed at the edge of the routing domain.
- A stub or NSSA can have multiple ABRs or exit points. However, all of the exit points and local routers must contain the same external routing data so that the exit point does not need to be determined for each external destination.

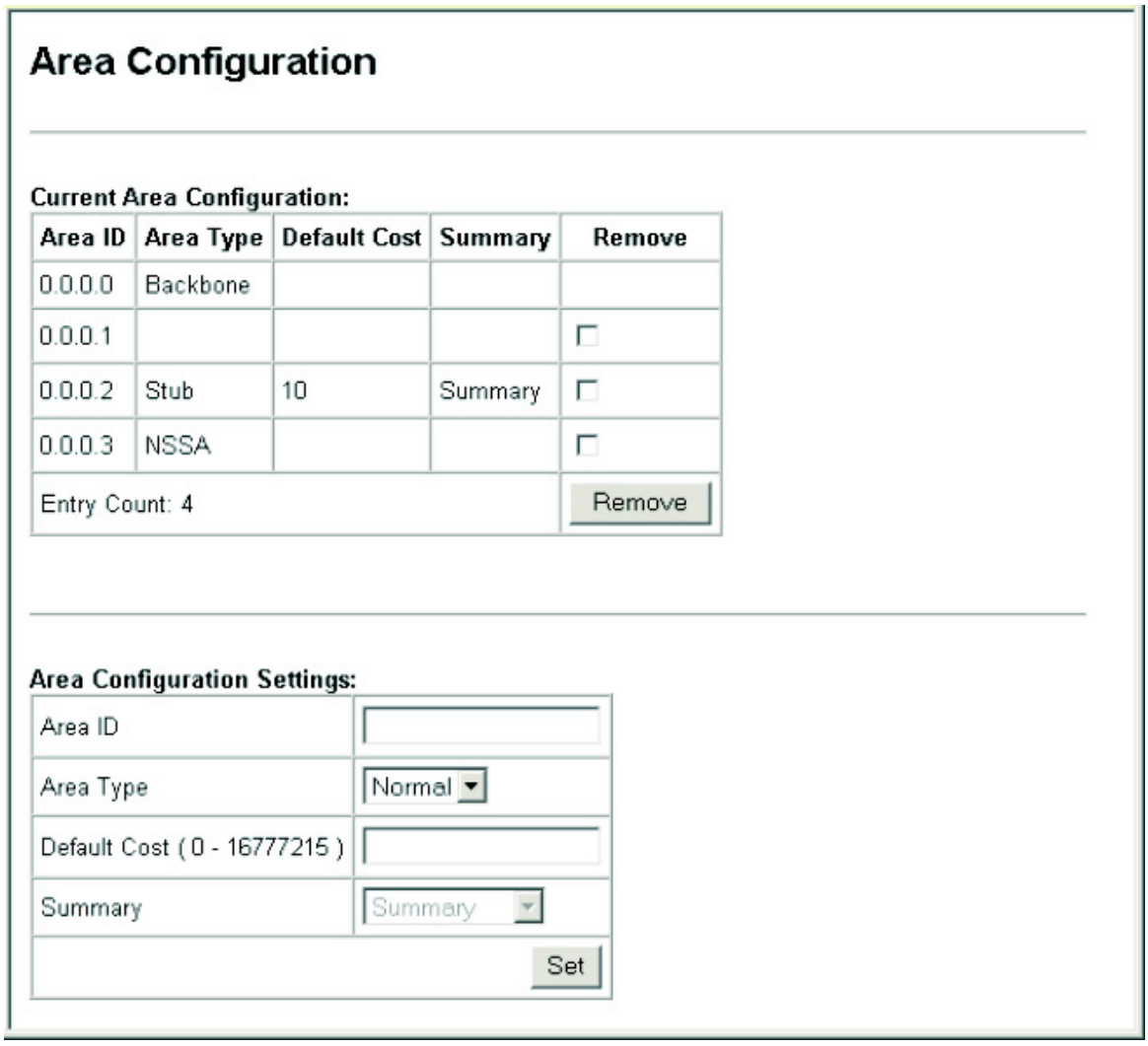
Command Attributes

- **Area ID** – Identifier for an area, stub or NSSA.
- **Area Type** – Specifies a normal area, stub area, or not-so-stubby area (NSSA). Area ID 0.0.0.0 is set to the backbone by default. (Default: Normal area)
- **Default Cost** – Cost for the default summary route sent into a stub from an area border router (ABR). (Range: 0-16777215; Default: 1)
  - Note that if you set the default cost to "0," the router will not advertise a default route into the attached stub.
- **Summary** – Makes an ABR send a Type-3 summary link advertisement into a stub. (Default: Summary)
  - A stub is designed to save routing table space by blocking Type-4 AS summary LSAs and Type 5 external LSAs. If you use the "NoSummary" option to also block Type-3 summary LSAs that advertise the default route for destinations external to the local area or the AS, the stub will become completely isolated.

Note: This router supports up to 16 total areas (either normal transit areas, stubs, or NSSAs).

Downloaded from www.Manualslib.com manuals search engine

Web - Click Routing Protocol, OSPF, Area Configuration. Set any area to a stub or NSSA as required, specify the cost for the default summary route sent into a stub, and click Apply.



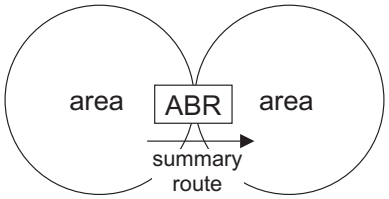
CLI - This example configures area 0.0.0.1 as a normal area, area 0.0.0.2 as a stub, and area 0.0.0.3 as an NSSA. It also configures the router to propagate a default summary route into the stub and sets the cost for this default route to 10.

```
Console(config-router)#network 10.1.1.0 255.255.255.0 area 0.0.0.13-155
Console(config-router)#area 0.0.0.2 stub summary3-156
Console(config-router)#area 0.0.0.2 default-cost 103-152
Console(config-router)#area 0.0.0.3 nssa3-158
Console(config-router)#end
```


Downloaded from www.Manualslib.com manuals search engine

```
Console#show ip ospf3-170
Routing Process with ID 192.168.1.253
Supports only single TOS(TOS0) route
Number of area in this router is 3
Area 0.0.0.0 (BACKBONE)
     Number of interfaces in this area is 1
     SPF algorithm executed 40 times
Area 0.0.0.2 (STUB)
     Number of interfaces in this area is 1
     SPF algorithm executed 8 times
Area 0.0.0.3 (NSSA)
     Number of interfaces in this area is 1
     SPF algorithm executed 40 times
Console#
```

Configuring Area Ranges (Route Summarization for ABRs)



An OSPF area can include a large number of nodes. If the Area Border Router (ABR) has to advertise route information for each of these nodes, this wastes a lot of bandwidth and processor time. Instead, you can configure an ABR to advertise a single summary route that covers all the individual networks within its area. When using route summaries, local changes do not have to be propagated to other area routers. This allows OSPF to be easily scaled for larger networks, and provides a more stable network topology.

Command Usage

- Use the Area Range Configuration page to summarize the routes for an area. The summary route for an area is defined by an IP address and network mask. You therefore need to structure each area with a contiguous set of addresses so that all routes in the area fall within an easily specified range. This router also supports Variable Length Subnet Masks (VLSMs), so you can summarize an address range on any bit boundary in a network address.

- To summarize the external LSAs imported into your autonomous system (i.e., local routing domain), use the Summary Address Configuration screen (page 3-308).

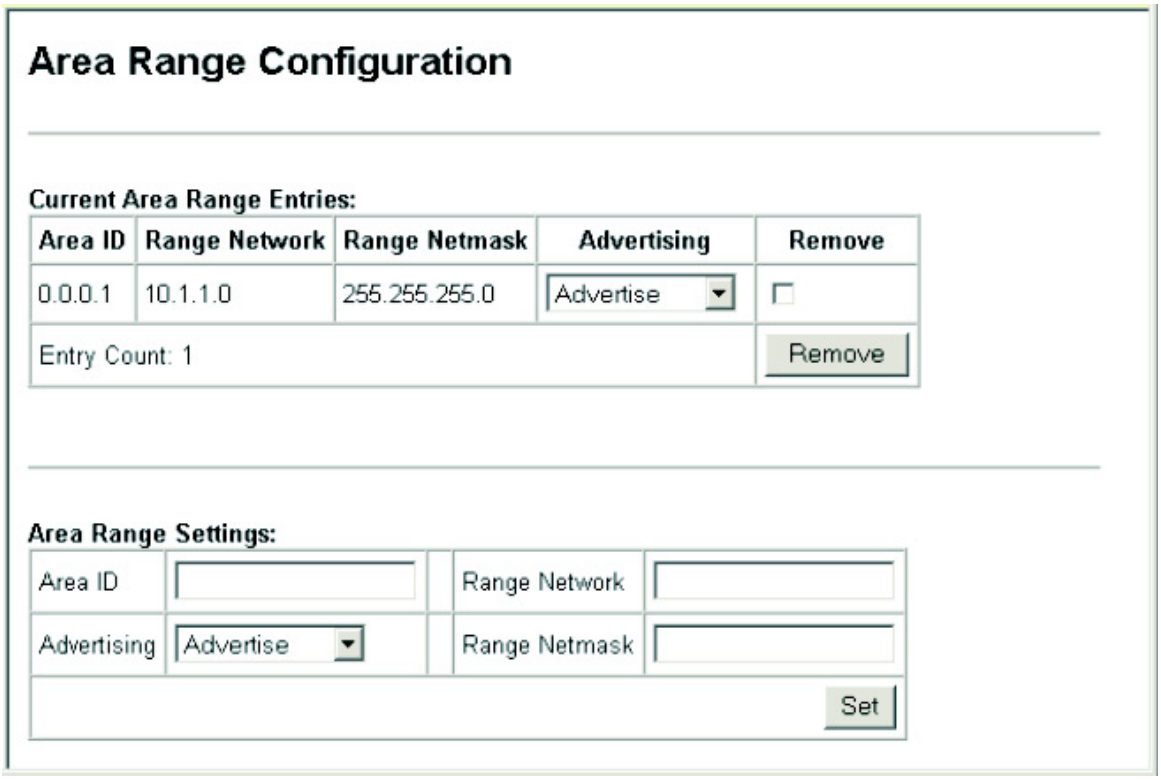
Downloaded from www.Manualslib.com manuals search engine

Command Attributes

- **Area ID** – Identifies an area for which the routes are summarized. (The area ID must be in the form of an IP address.)
- **Range Network** – Base address for the routes to summarize.
- **Range Netmask** – Network mask for the summary route.
- **Advertising** – Indicates whether or not to advertise the summary route. If the summary is not sent, the routes remain hidden from the rest of the network. (Default: Advertise)

Note: This router supports up 64 summary routes for area ranges.

Web - Click Routing Protocol, OSPF, Area Range Configuration. Specify the area identifier, the base address and network mask, select whether or not to advertise the summary route to other areas, and then click Apply.



CLI - This example summarizes all the routes for area 1. Note that the default for the **area range** command is to advertise the route summary.

Downloaded from www.Manualslib.com manuals search engine

The configured summary route is shown in the list of information displayed for area 1.

```
Console(config-router)#area 0.0.0.1 range 10.1.1.0 255.255.255.03-155
Console(config-router)#end
Console#show ip ospf
Routing Process with ID 10.1.1.253
Supports only single TOS(TOS0) route
Number of area in this router is 4
Area 0.0.0.0 (BACKBONE)
     Number of interfaces in this area is 0
     SPF algorithm executed 47 times
Area 0.0.0.1
     Number of interfaces in this area is 3
     SPF algorithm executed 14 times
     Area ranges are
        255.255.255.0/24  Active
Console#
```

Configuring OSPF Interfaces

You should specify a routing interface for any local subnet that needs to communicate with other network segments located on this router or elsewhere in the network. First configure a VLAN for each subnet that will be directly connected to this router, assign IP interfaces to each VLAN (i.e., one primary interface and one or more secondary interfaces), and then use the OSPF / Network Area Address Configuration page to assign an interface address range to an OSPF area.

After assigning a routing interface to an OSPF area, you need to use the OSPF / Interface Configuration page to configure the interface-specific parameters used by OSPF to select the designated router, control the timing of link state advertisements, set the cost used to select preferred paths, and specify the method used to authenticate routing messages.

Field Attributes

OSPF Interface List

- **VLAN ID** – The VLAN to which an IP interface has been assigned.
- **Interface IP** – The IP interface associated with the selected VLAN.
- **Area ID** – The area to which this interface has been assigned.

Downloaded from www.Manualslib.com manuals search engine

- **Designated Router** – Designated router for this area.
- **Backup Designated Router** – Designated backup router for this area.
- **Entry Count** – The number of IP interfaces assigned to this VLAN.

Note: This router supports up 64 OSPF interfaces.

Detail Interface Configuration

- **VLAN ID** – The VLAN corresponding to the selected interface.
- **Rtr Priority** – Sets the interface priority for this router. (Range: 0-255; Default: 1)
  - A designated router (DR) and backup designated router (BDR) is elected for each OSPF area based on Router Priority. The DR forms an active adjacency to all other routers in the area to exchange routing topology information. If for any reason the DR fails, the BDR takes over this role.
  - The router with the highest priority becomes the DR and the router with the next highest priority becomes the BDR. If two or more routers are set to the same priority, the router with the higher ID will be elected. You can set the priority to zero to prevent a router from being elected as a DR or BDR.
  - If a DR already exists for an area when this interface comes up, the new router will accept the current DR regardless of its own priority. The DR will not change until the next time the election process is initiated.
- **Transmit Delay** – Sets the estimated time to send a link-state update packet over an interface. (Range: 1-65535 seconds; Default: 1)
  - LSAs have their age incremented by a delay before transmission. You should consider both the transmission and propagation delays for an interface when estimating this delay. Set the transmit delay according to link speed, using larger values for lower-speed links.

Downloaded from www.Manualslib.com manuals search engine

- The transmit delay must be the same for all routers in an autonomous system.
- On slow links, the router may send packets more quickly than devices can receive them. To avoid this problem, you can use the transmit delay to force the router to wait a specified interval between transmissions.

- **Retransmit Interval** – Sets the time between resending link-state advertisements. (Range: 1-65535 seconds; Default: 1)
  - A router will resend an LSA to a neighbor if it receives no acknowledgment. The retransmit interval should be set to a conservative value that provides an adequate flow of routing information, but does not produce unnecessary protocol traffic. Note that this value should be larger for virtual links.
  - Set this interval to a value that is greater than the round-trip delay between any two routers on the attached network to avoid unnecessary retransmissions.

- **Hello Interval** – Sets the interval between sending hello packets on an interface. (Range: 1-65535 seconds; Default: 10)
  - This interval must be set to the same value for all routers on the network.
  - Using a smaller Hello interval allows changes in the network topology to be discovered more quickly, but may result in more routing traffic.

- **Rtr Dead Interval** – Sets the interval at which hello packets are not seen before neighbors declare the router down. This interval must be set to the same value for all routers on the network. (Range: 1-65535 seconds; Default: 40, or 4 times the Hello Interval)

- **Cost** – Sets the cost of sending a packet on an interface, where higher values indicate slower ports. (Range: 1-65535; Default: 1)
  - This router uses a default cost of 1 for all ports. Therefore, if you install a Gigabit module, you need to reset the cost for all of the 100 Mbps ports to some value greater than 1.

Downloaded from www.Manualslib.com manuals search engine

- Routes are subsequently assigned a metric equal to the sum of all metrics for each interface link in the route.

- **Authentication Type** – Specifies the authentication type used for an interface. (Options: None, Simple password, MD5; Default: None)
  - Use authentication to prevent routers from inadvertently joining an unauthorized area. Configure routers in the same area with the same password or key.
  - When using simple password authentication, a password is included in the packet. If it does not match the password configured on the receiving router, the packet is discarded. This method provides very little security as it is possible to learn the authentication key by snooping on routing protocol packets.
  - When using Message-Digest 5 (MD5) authentication, the router uses the MD5 algorithm to verify data integrity by creating a 128-bit message digest from the authentication key. Without the proper key and key-id, it is nearly impossible to produce any message that matches the prespecified target message digest.
  - The Authentication Key and Message Digest Key-id must be used consistently throughout the autonomous system. (Note that the Message Digest Key-id field is disabled when this authentication type is selected.)

- **Authentication Key** – Assign a plain-text password used by neighboring routers to verify the authenticity of routing protocol messages. (Range: 1-8 characters for simple password or 1-16 characters for MD5 authentication; Default: no key)

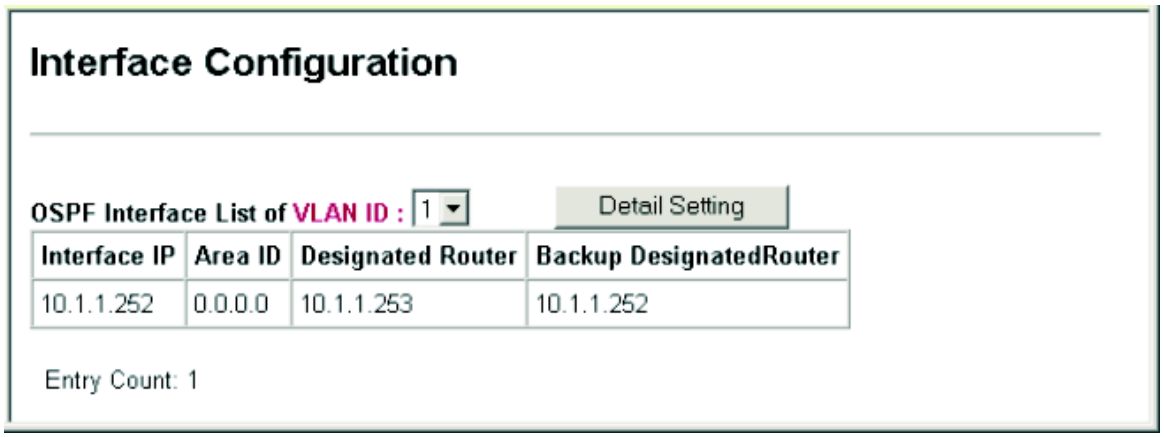
  - You can assign a unique password to each network (i.e., autonomous system) to improve the security of the routing database. However, the password must be used consistently on all neighboring routers throughout a network.

- **Message Digest Key-id** – Assigns a key-id used in conjunction with the authentication key to verify the authenticity of routing protocol messages sent to neighboring routers. (Range: 1-255; Default: none)

Downloaded from www.Manualslib.com manuals search engine

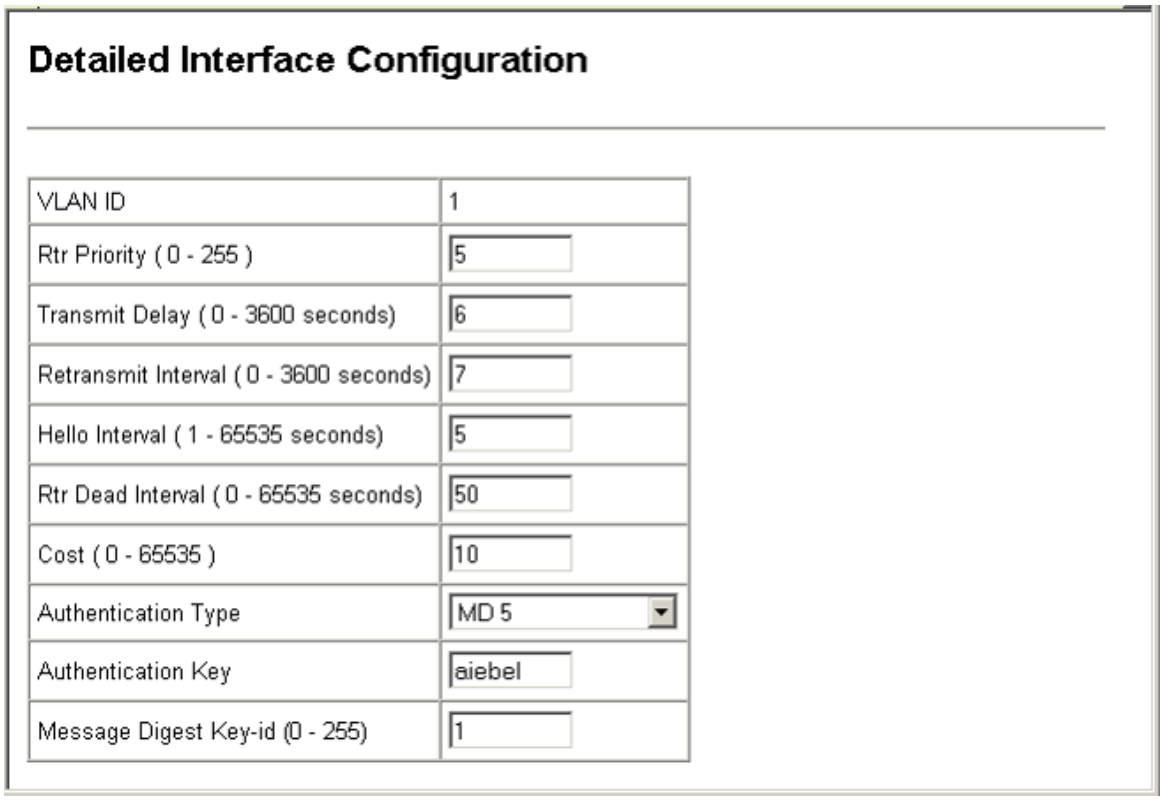
- Normally, only one key is used per interface to generate authentication information for outbound packets and to authenticate incoming packets. Neighbor routers must use the same key identifier and key value.
- When changing to a new key, the router will send multiple copies of all protocol messages, one with the old key and another with the new key. Once all the neighboring routers start sending protocol messages back to this router with the new key, the router will stop using the old key. This rollover process gives the network administrator time to update all the routers on the network without affecting the network connectivity. Once all the network routers have been updated with the new key, the old key should be removed for security reasons.

Web - Click Routing Protocol, OSPF, Interface Configuration. Select the required interface from the scroll-down box, and click Detailed Settings.



Downloaded from www.Manualslib.com manuals search engine

Change any of the interface-specific protocol parameters, and then click Apply.

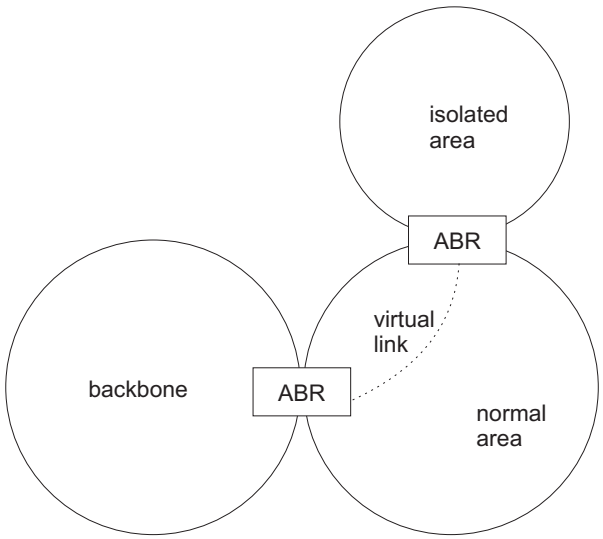


CLI - This example configures the interface parameters for VLAN 1.

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf priority 53-168
Console(config-if)#ip ospf transmit-delay 63-169
Console(config-if)#ip ospf retransmit-interval 73-169
Console(config-if)#ip ospf hello-interval 53-167
Console(config-if)#ip ospf dead-interval 503-166
Console(config-if)#ip ospf cost 103-166
Console(config-if)#ip ospf authentication message-digest3-163
Console(config-if)#ip ospf message-digest-key 1 md5 aiebel3-165
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Configuring Virtual Links



All OSPF areas must connect to the backbone. If an area does not have a direct physical connection to the backbone, you can configure a virtual link that provides a logical path to the backbone. To connect an isolated area to the backbone, the logical path can cross a single non-backbone area (i.e., transit area) to reach the backbone. To define this path, you must configure an ABR that serves as an endpoint connecting the isolated area to the common transit area, and specify a neighboring ABR as the other endpoint connecting the common transit area to the backbone itself. (Note that you cannot configure a virtual link that runs through a stub or NSSA area.)

Virtual links can also be used to create a redundant link between any area and the backbone to help prevent partitioning, or to connect two existing backbone areas into a common backbone.

Command Attributes

- **Area ID** – Identifies the transit area for the virtual link. (The area ID must be in the form of an IP address.)

- **Neighbor Router ID** – Neighbor router at other end of the virtual link. This must be an Area Border Router (ABR) that is adjacent to both the backbone and the transit area for the virtual link.

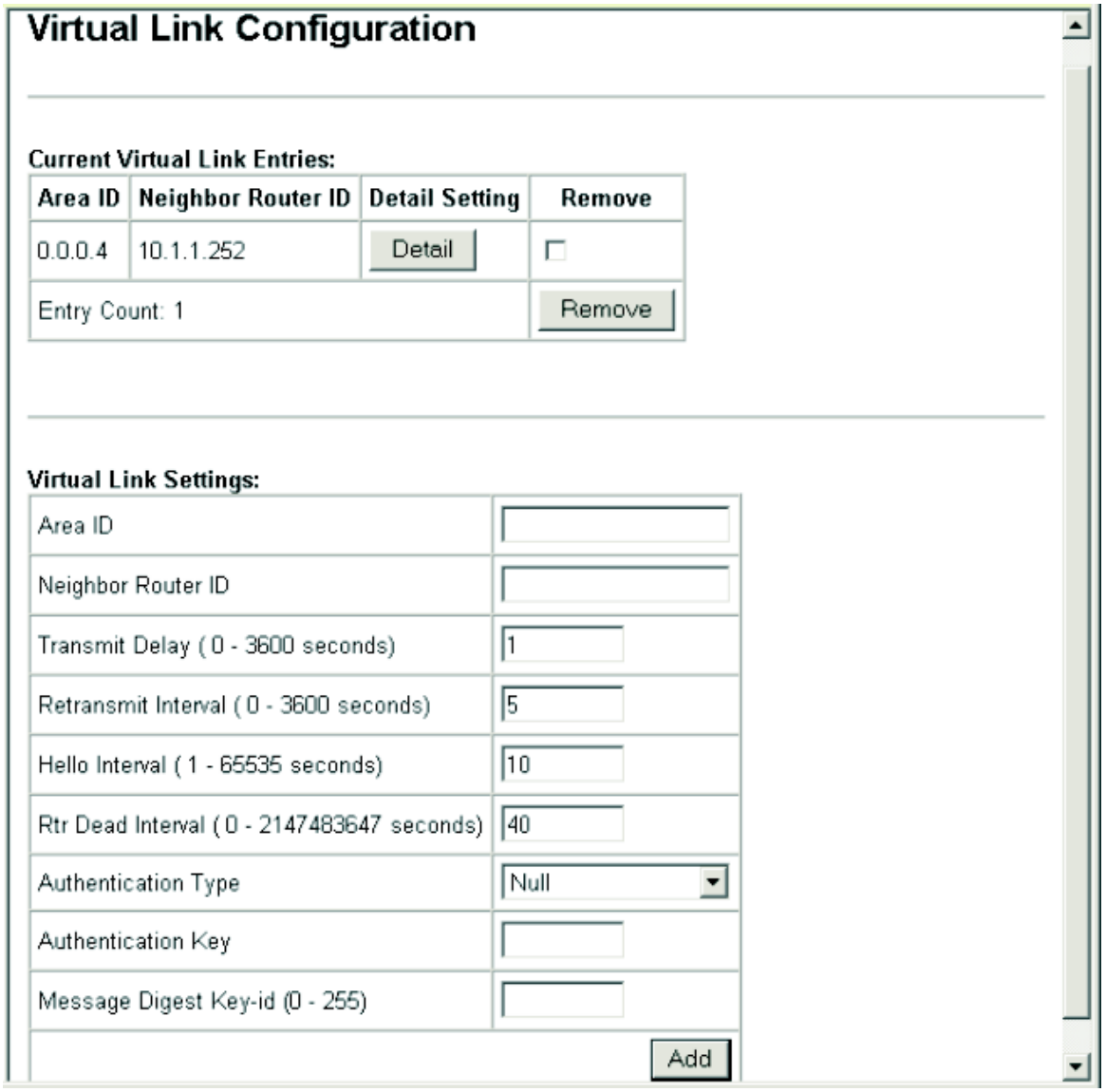
- **Events** – The number of state changes or error events on this virtual link.

The other items are described under "Configuring OSPF Interfaces," page 3-297.

Downloaded from www.Manualslib.com manuals search engine

Note: This router supports up 64 virtual links.

Web - Click Routing Protocol, OSPF, Virtual Link Configuration. To create a new virtual link, specify the Area ID and Neighbor Router ID, configure the link attributes, and click Add. To modify the settings for an existing link, click the Detail button for the required entry, modify the link settings, and click Set.



Downloaded from www.Manualslib.com manuals search engine

CLI - This example configures a virtual link from the ABR adjacent to area 0.0.0.4, through a transit area to the neighbor router 10.1.1.252 at the other end of the link which is adjacent to the backbone.

```
Console(config-router)#area 0.0.0.0 virtual-link 10.1.1.2523-160
Console(config-router)#
```

Configuring Network Area Addresses

OSPF protocol broadcast messages (i.e., Link State Advertisements or LSAs) are restricted by area to limit their impact on network performance. A large network should be split up into separate OSPF areas to increase network stability, and to reduce protocol traffic by summarizing routing information into more compact messages. Each router in an area shares the same view of the network topology, including area links, route summaries for directly connected areas, and external links to other areas.

Command Usage

- Use the Network Area Address Configuration page to specify an Area ID and the corresponding network address range. Each area identifies a logical group of OSPF routers that actively exchange LSAs to ensure that they share an identical view of the network topology.

- Each area must be connected to a backbone area. This area passes routing information between other areas in the autonomous system. The default value 0.0.0.0 is used as the Area ID for the backbone. All routers must be connected to the backbone, either directly, or through a virtual link if a direct physical connection is not possible.

- An area initially configured via the Network Area Address Configuration page is set as a normal area (or transit area) by default. A normal area can send and receive external Link State Advertisements (LSAs). If necessary, you can use the Area Configuration page to configure an area as a stubby area that cannot send or receive external LSAs, or a not-so-stubby area (NSSA) that can import external route information into its area (page 3-291).

Downloaded from www.Manualslib.com manuals search engine

- An area must be assigned a range of subnetwork addresses. This area and the corresponding address range forms a routing interface, and can be configured to aggregate LSAs from all of its subnetwork addresses and exchange this information with other routers in the network (page 3-295).

Command Attributes

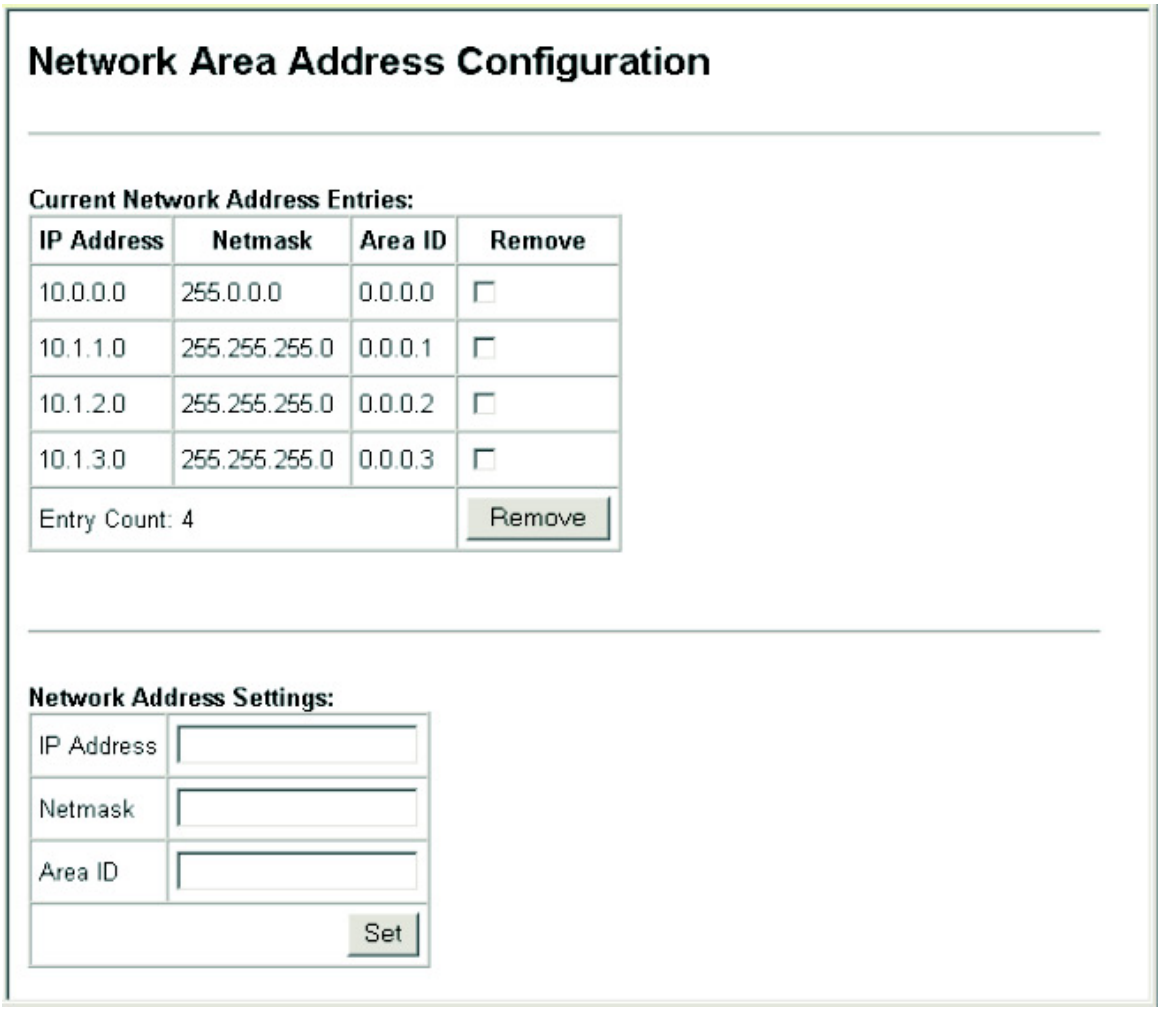
- **IP Address** – Address of the interfaces to add to the area.
- **Netmask** – Network mask of the address range to add to the area.
- **Area ID** – Area to which the specified address or range is assigned. An OSPF area identifies a group of routers that share common routing information. (The area ID must be in the form of an IP address.)

Note: This router supports up to 16 total areas (either normal transit areas, stubs, or NSSAs).

Web - Click Routing Protocol, OSPF, Network Area Address Configuration. Configure a backbone area that is contiguous with all the

Downloaded from www.Manualslib.com manuals search engine

other areas in your network, configure an area for all of the other OSPF interfaces, then click Apply.



Downloaded from www.Manualslib.com manuals search engine

CLI - This example configures the backbone area and one transit area.

```
Console(config-router)#network 10.0.0.0 255.0.0.0 area 0.0.0.03-155
Console(config-router)#network 10.1.1.0 255.255.255.0 area 0.0.0.1
Console(config-router)#end
Console#show ip ospf3-170
Routing Process with ID 10.1.1.253
Supports only single TOS(TOS0) route
Number of area in this router is 4
Area 0.0.0.0 (BACKBONE)
     Number of interfaces in this area is 1
     SPF algorithm executed 8 times
Area 0.0.0.1
     Number of interfaces in this area is 1
     SPF algorithm executed 5 times
Area 0.0.0.2 (STUB)
     Number of interfaces in this area is 1
     SPF algorithm executed 13 times
Area 0.0.0.3 (NSSA)
     Number of interfaces in this area is 1
     SPF algorithm executed 12 times
Console#
```

Configuring Summary Addresses (for External AS Routes)

An Autonomous System Boundary Router (ASBR) can redistribute routes learned from other protocols into all attached autonomous systems. (See "Redistributing External Routes" on page 3-310) To reduce the amount of external LSAs imported into your local routing domain, you can configure the router to advertise an aggregate route that consolidates a broad range of external addresses.

Command Usage

- If you are not sure what address ranges to consolidate, first enable external route redistribution via the Redistribute Configuration screen, view the routes imported into the routing table, and then configure one or more summary addresses to reduce the size of the routing table and consolidate these external routes for advertising into the local domain.

- To summarize routes sent between OSPF areas, use the Area Range Configuration screen (page 3-295).

Command Attributes

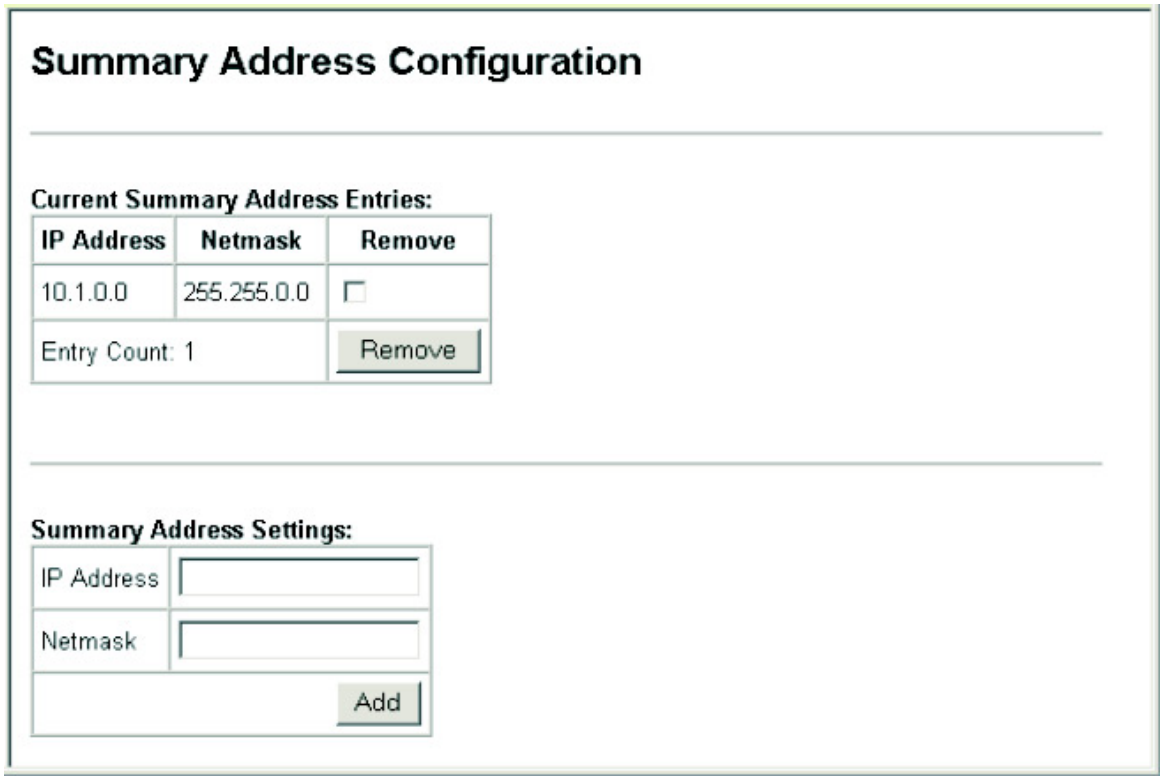
- **IP Address** – Summary address covering a range of addresses.

Downloaded from www.Manualslib.com manuals search engine

- **Netmask** – Network mask for the summary route.

Note: This router supports up 16 Type-5 summary routes.

Web - Click Routing Protocol, OSPF, Summary Address Configuration. Specify the base address and network mask, then click Add.



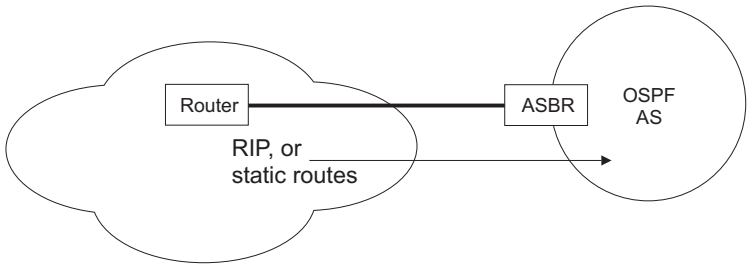
CLI - This example This example creates a summary address for all routes contained in 192.168.x.x.

```
Console(config-router)#summary-address 192.168.0.0 255.255.0.03-153
Console(config-router)#
```


Downloaded from www.Manualslib.com manuals search engine

Redistributing External Routes

You can configure this router to import external routing information from other routing protocols into the autonomous system.



Command Usage

- This router supports redistribution for both RIP and static routes.
- When you redistribute external routes into an OSPF autonomous system (AS), the router automatically becomes an autonomous system boundary router (ASBR).
- However, if the router has been manually configured as an ASBR via the General Configuration screen, but redistribution is not enabled, the router will only generate a "default" external route into the AS if it has been configured to "always" advertise a default route even if an external route does not actually exist (page 3-287).
- Metric type specifies the way to advertise routes to destinations outside the autonomous system (AS) via External LSAs. Specify Type 1 to add the internal cost metric to the external route metric. In other words, the cost of the route from any router within the AS is equal to the cost associated with reaching the advertising ASBR, plus the cost of the external route. Specify Type 2 to only advertise external route metric.
- The metric value specified for redistributed routes supersedes the Default External Metric specified in the OSPF / General Configuration screen (page 3-287).

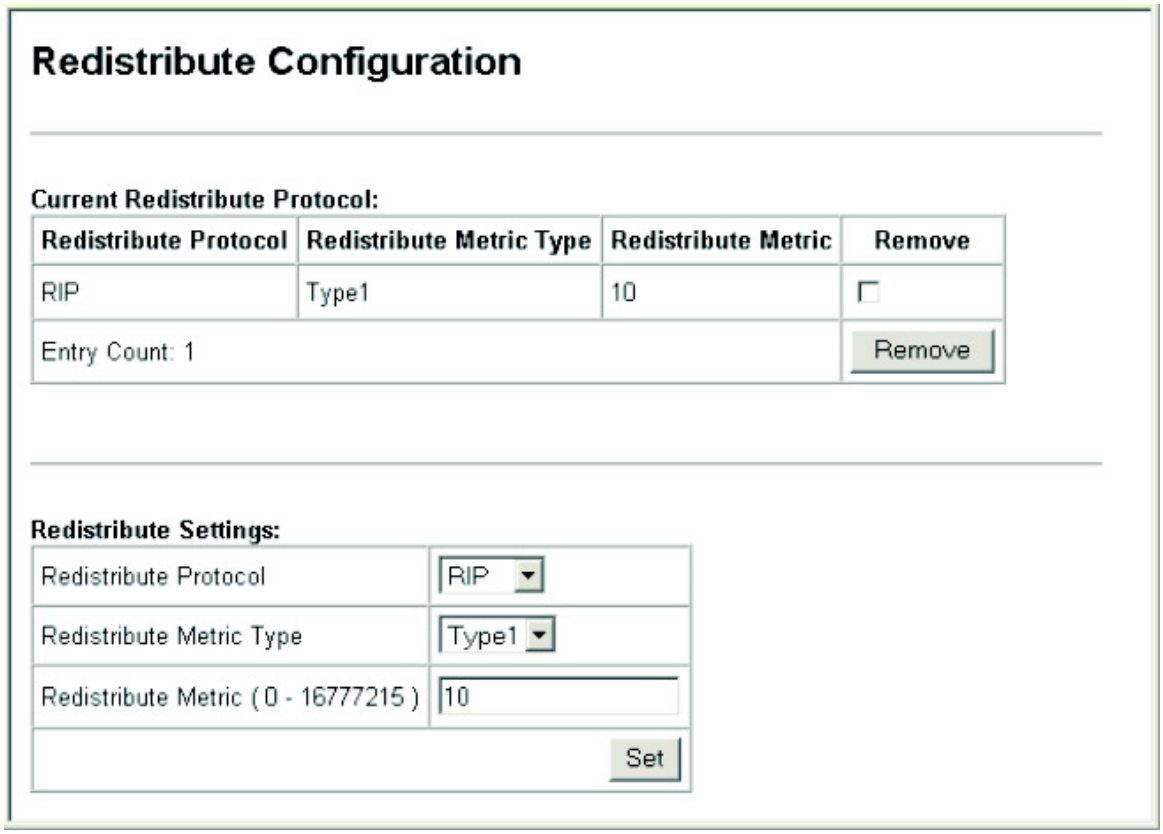
Command Attributes

- **Redistribute Protocol** – Specifies the external routing protocol type for which routing information is to be redistributed into the local routing domain. (Options: RIP, Static; Default: RIP)

Downloaded from www.Manualslib.com manuals search engine

- **Redistribute Metric Type** – Indicates the method used to calculate external route costs. (Options: Type 1, Type 2; Default: Type 1)
- **Redistribute Metric** – Metric assigned to all external routes for the specified protocol. (Range: 1-65535: Default: 10)

Web - Click Routing Protocol, OSPF, Redistribute. Specify the protocol type to import, the metric type and path cost, then click Add.



CLI - This example redistributes routes learned from RIP as Type 1 external routes.

```
Console(config-router)#redistribute rip metric-type 13-154
Console(config-router)#
```

Configuring NSSA Settings

Use the OSPF / NSSA Settings page to configure a not-so-stubby area (NSSA), and to control the use of default routes for ABRs and ASBRs, or external routes learned from other routing domains and imported via an

Downloaded from www.Manualslib.com manuals search engine

ABR. (For a detailed description of NSSA areas, refer to "Configuring OSPF Areas" on page 3-291.)

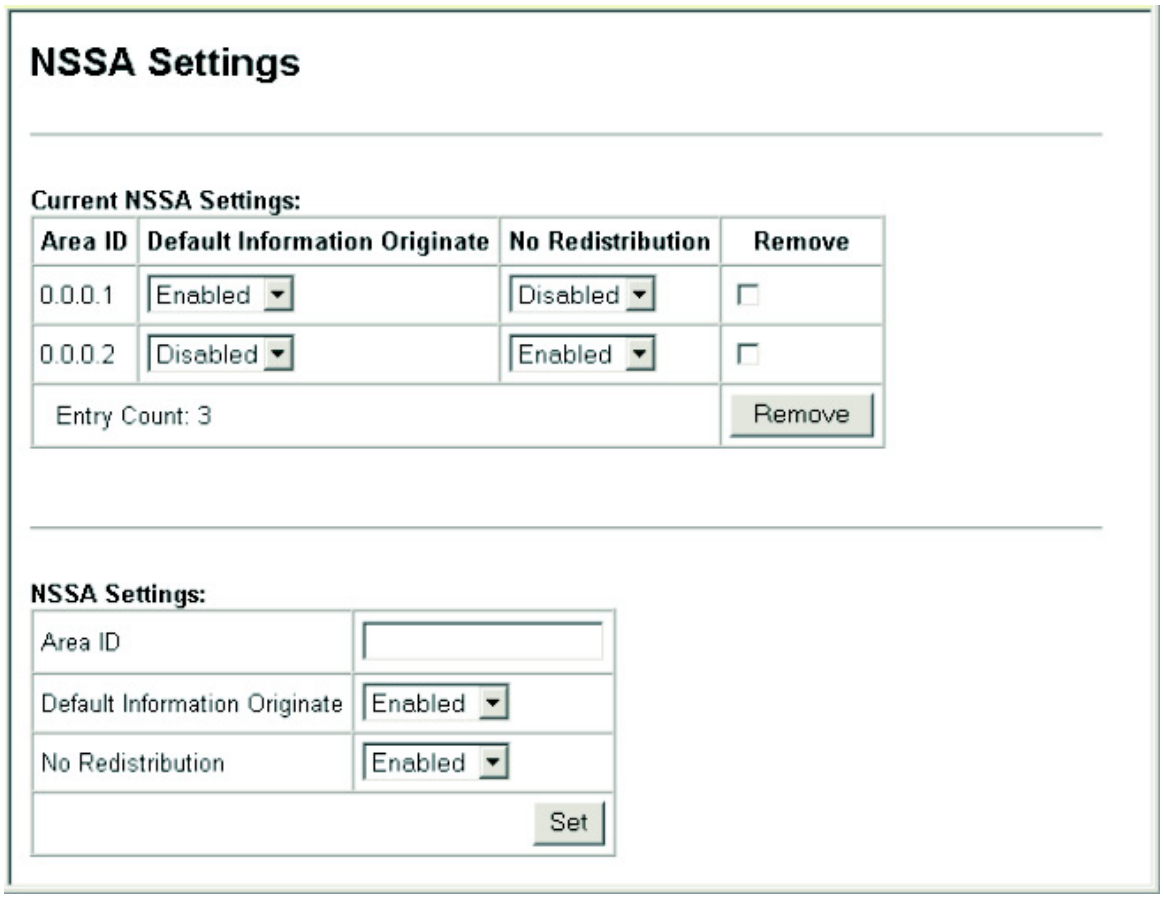
Command Attributes

- **Area ID** – Identifier for an not-so-stubby area (NSSA).
- **Default Information Originate** – An NSSA ASBR originates and floods Type-7 external LSAs throughout its area for known network destination outside of the AS. However, you can also configure an NSSA ASBR to generate a Type-7 "default" route to areas outside of the AS, or an NSSA ABR to generate a Type-7 "default" route to other areas within the AS. (Default: Disabled)
- **No Redistribution** – The Redistribute Configuration page (page 3-310) is used to import information from other routing domains (or protocols) into the AS. However, when the router is an NSSA ABR, you can choose whether or not to accept external routes learned from routers in other OSPF areas into the NSSA. (Default: Enabled)

Note: This router supports up 16 areas, either normal transit areas, stubs, or NSSAs.

Downloaded from www.Manualslib.com manuals search engine

Web - Click Routing Protocol, OSPF, NSSA Settings. Create a new NSSA or modify the routing behavior for an existing NSSA, and click Apply.



CLI - This example configures area 0.0.0.1 as a stub and sets the cost for the default summary route to 10.

```
Console(config-router)#area 0.0.0.1 nssa
default-information- originate3-158
Console(config-router)#area 0.0.0.2 nssa no-redistribution 3-158
Console(config-router)#
```

Displaying Link State Database Information

OSPF routers advertise routes using Link State Advertisements (LSAs). The full collection of LSAs collected by a router interface from the attached area is known as a link state database. Routers that are connected to multiple interfaces will have a separate database for each area. Each router in the same area should have an identical database describing the topology for that area, and the shortest path to external destinations.

Downloaded from www.Manualslib.com manuals search engine

The full database is exchanged between neighboring routers as soon as a new router is discovered. Afterwards, any changes that occur in the routing tables are synchronized with neighboring routers through a process called reliable flooding. You can show information about different LSAs stored in this router's database, which may include any of the following types:

- Router (Type 1) – All routers in an OSPF area originate Router LSAs that describe the state and cost of its active interfaces and neighbors.
- Network (Type 2) – The designated router for each area originates a Network LSA that describes all the routers that are attached to this network segment.
- Summary (Type 3) – Area border routers can generate Summary LSAs that give the cost to a subnetwork located outside the area.
- AS Summary (Type 4) – Area border routers can generate AS Summary LSAs that give the cost to an autonomous system boundary router (ASBR).
- AS External (Type 5) – An ASBR can generate an AS External LSA for each known network destination outside the AS.
- NSSA External (Type 7) – An ASBR within an NSSA generates an NSSA external link state advertisement for each known network destination outside the AS.

Command Attributes

- **Area ID** – Area defined for which you want to view LSA information. (This item must be entered in the form of an IP address.)
- **Link ID** – The network portion described by an LSA. The Link ID should be:
  - An IP network number for Type 3 Summary and Type 5 AS External LSAs. (When an Type 5 AS External LSA is describing a default route, its Link ID is set to the default destination 0.0.0.0.)

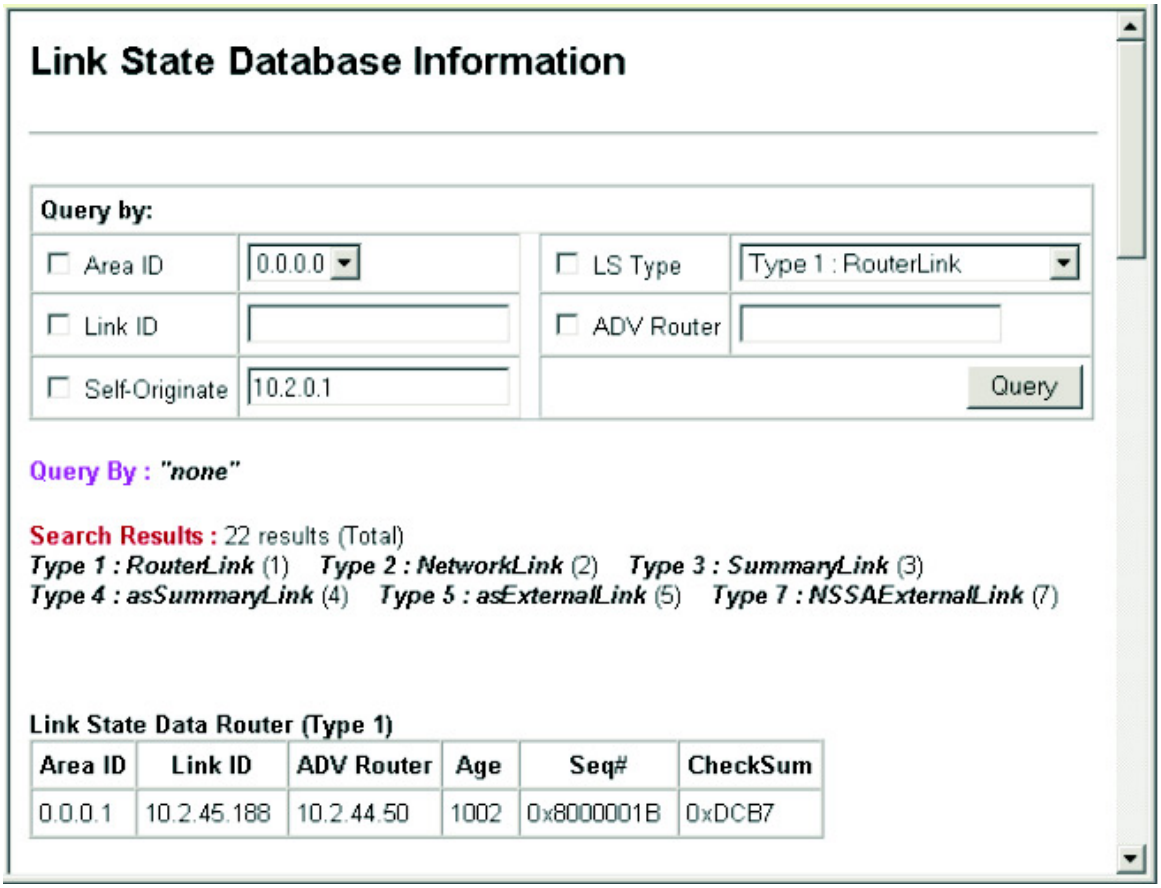
Downloaded from www.Manualslib.com manuals search engine

  - A Router ID for Router, Network, and Type 4 AS Summary LSAs.
- **Self-Originate** – Shows LSAs originated by this router.
- **LS Type** – LSA Type (Options: Type 1-5, 7). See the preceding description.
- **Adv Router** – IP address of the advertising router. If not entered, information about all advertising routers is displayed.
- **Age*** – Age of LSA (in seconds).
- **Seq*** – Sequence number of LSA (used to detect older duplicate LSAs).
- **CheckSum*** – Checksum of the complete contents of the LSA.

* These items are read only.

Downloaded from www.Manualslib.com manuals search engine

Web - Click Routing Protocol, OSPF, Link State Database Information. Specify parameters for the LSAs you want to display, then click Query.



CLI - The CLI provides a wider selection of display options for viewing the Link State Database. See "show ip ospf database" on page 3-172.

Displaying Information on Border Routers

You can display entries in the local routing table for Area Border Routers (ABR) and Autonomous System Boundary Routers (ASBR) known by this device.

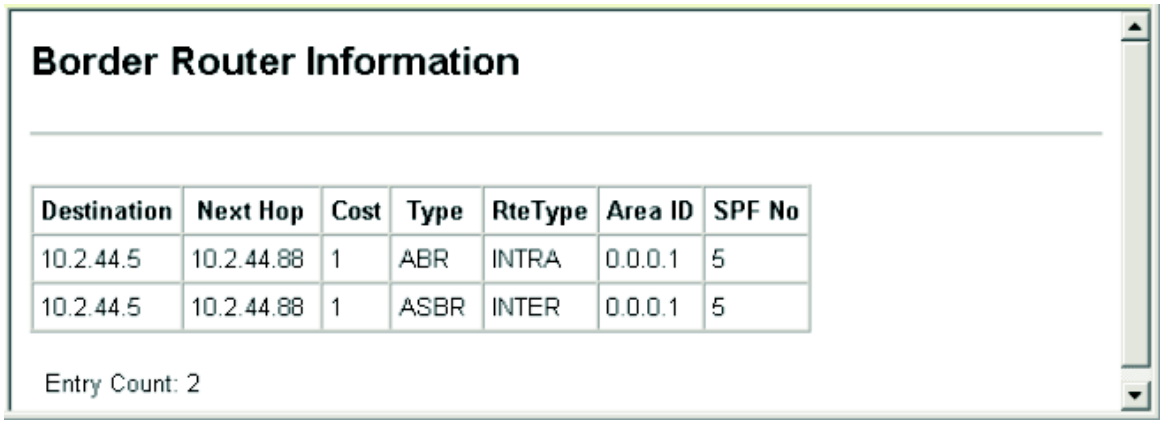
Field Attributes

- **Destination** – Identifier for the destination router.
- **Next Hop** – IP address of the next hop toward the destination.
- **Cost** – Link metric for this route.

Downloaded from www.Manualslib.com manuals search engine

- **Type** – Router type of the destination; either ABR, ASBR or both.
- **Rte Type** – Route type; either intra-area or interarea route (INTRA or INTER).
- **Area** – The area from which this route was learned.
- **SPF No** – The number of times the shortest path first algorithm has been executed for this route.

Web - Click Routing Protocol, OSPF, Border Router Information.



Border Router Information

Destination	Next Hop	Cost	Type	RteType	Area ID	SPF No
10.2.44.5	10.2.44.88	1	ABR	INTRA	0.0.0.1	5
10.2.44.5	10.2.44.88	1	ASBR	INTER	0.0.0.1	5

Entry Count: 2

CLI - This example shows one router that serves as both the ABR for the local area and the ASBR for the autonomous system.

```
Console#show ip ospf border-routers3-171

  Destination      Next Hop      Cost   Type  RteType      Area        SPF No
--------------- --------------- ------ ----- -------- ---------------
-------
     10.2.44.5      10.2.44.88      1   ABR    INTRA         0.0.0.1       5
     10.2.44.5      10.2.44.88      1   ASBR   INTER         0.0.0.1       5
Console#
```

Displaying Information on Neighbor Routers

You can display about neighboring routers on each interface within an OSPF area.

Field Attributes

- **ID** – Neighbor's router ID.

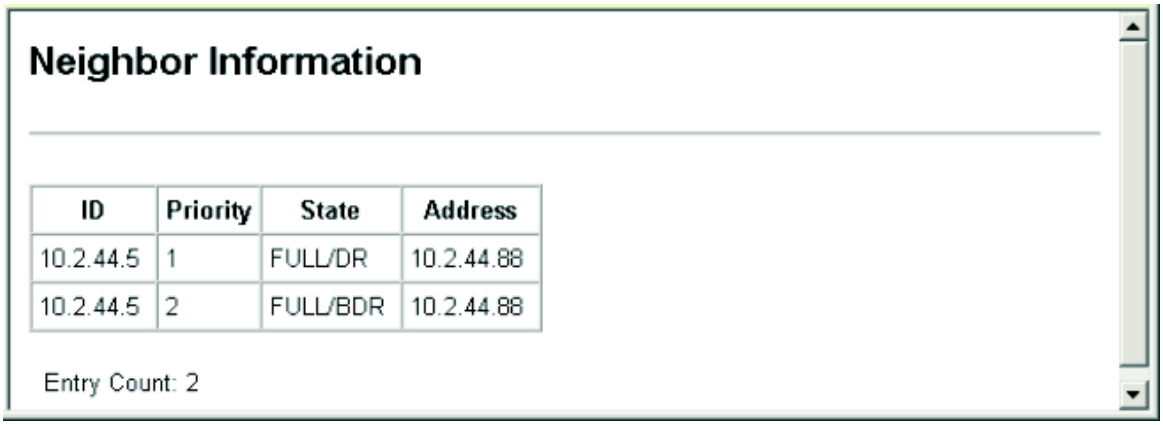
Downloaded from www.Manualslib.com manuals search engine

- **Priority** – Neighbor's router priority.
- **State** – OSPF state and identification flag.

  States include:
  - Down – Connection down
  - Attempt – Connection down, but attempting contact (non-broadcast networks)
  - Init – Have received Hello packet, but communications not yet established
  - Two-way – Bidirectional communications established
  - ExStart – Initializing adjacency between neighbors
  - Exchange – Database descriptions being exchanged
  - Loading – LSA databases being exchanged
  - Full – Neighboring routers now fully adjacent

  Identification flags include:
  - D – Dynamic neighbor
  - S – Static neighbor
  - DR – Designated router
  - BDR – Backup designated router
- **Address** – IP address of this interface.

Web - Click Routing Protocol, OSPF, Neighbor Information.



CLI - This shows a designated router and backup designated router as

Downloaded from www.Manualslib.com manuals search engine

neighbors.

```
Console#show ip ospf neighbor3-182

      ID          Pri        State          Address
--------------- ------ ---------------- ---------------
      10.2.44.5      1          FULL/DR      10.2.44.88
      10.2.44.6      2         FULL/BDR      10.2.44.88

Console#
```

Multicast Routing

This router can route multicast traffic to different subnetworks using either Distance Vector Multicast Routing Protocol (DVMRP) or Protocol-Independent Multicasting - Dense Mode (PIM-DM). These protocols flood multicast traffic downstream, and calculate the shortest-path, source-rooted delivery tree between each source and destination host group. They also rely on messages sent from IGMP-enabled Layer 2 switches and hosts to determine when hosts want to join or leave multicast groups.

DVMRP builds a source-rooted multicast delivery tree that allows it to prevent looping and determine the shortest path to the source of the multicast traffic. PIM also builds a source-rooted multicast delivery tree for each multicast source, but uses information from the router's unicast routing table instead of maintaining its own multicast routing table, making it routing protocol independent. Also note that the Dense Mode version of PIM is supported on this router because it is suitable for densely populated multicast groups which occur primarily in the LAN environment.

If DVMRP and PIM-DM are not enabled on this router or another multicast routing protocol is used on your network, you can manually configure the switch ports attached to a multicast router (page 3-196).

Configuring Global Settings for Multicast Routing

To use multicast routing on this router, you must first globally enable multicast routing as described in this section, globally enable DVRMP

Downloaded from www.Manualslib.com manuals search engine

(page 3-324) or PIM (page 3-335), and specify the interfaces that will participate (page 3-329 or 3-336). Note that you can only enable one multicast routing protocol on any given interface.

Web – Click IP, Multicast Routing, General Setting. Set Multicast Forwarding Status to Enabled, and click Apply.

CLI – This example enables multicast routing globally for the router.

```
Console(config)#ip multicast-routing3-187
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

Displaying the Multicast Routing Table

You can display information on each multicast route this router has learned via DVMRP or PIM. The router learns multicast routes from neighboring routers, and also advertises these routes to its neighbors. The router stores entries for all paths learned by itself or from other routers, without considering actual group membership or prune messages. The routing table therefore does not indicate that the router has processed multicast traffic from any particular source listed in the table. It uses these routes to forward multicast traffic only if group members appear on directly-attached subnetworks or on subnetworks attached to downstream routers.

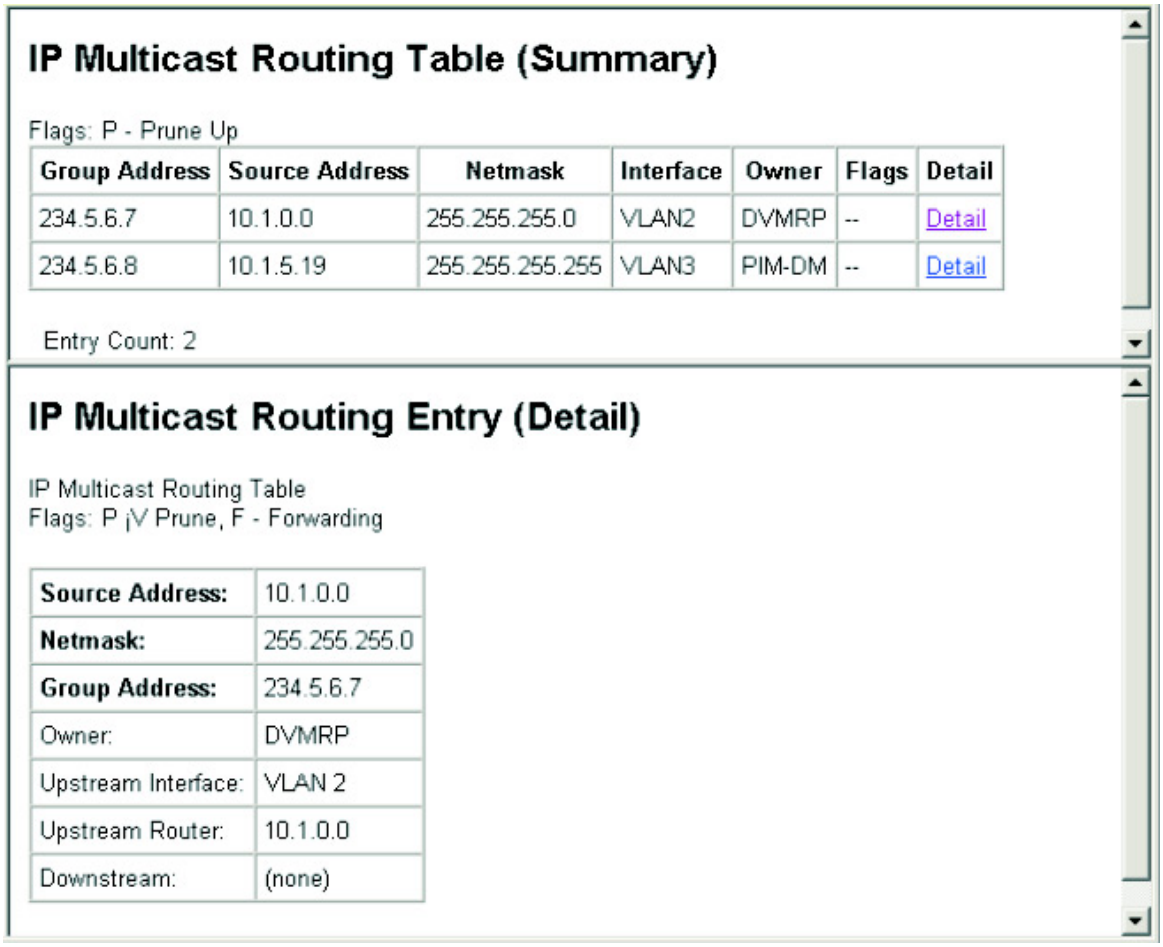
Field Attributes

- **Group Address** – IP group address for a multicast service.
- **Source Address** – Subnetwork containing the IP multicast source.
- **Netmask** – Network mask for the IP multicast source.
- **Interface** – Interface leading to the upstream neighbor.
- **Owner** – The associated multicast protocol (i.e., DVMRP or PIM).
- **Flags** – The flags associated with each interface indicate prune (P) if the downstream interface has been recently terminated or forwarding (F) if the interface is still active.
- **Detail** – This button displays detailed information for the selected entry.
- **Upstream Router*** – The multicast router immediately upstream for this group.
- **Downstream*** – Interface(s) on which multicast subscribers have been recorded.

* These items are displayed in the IP Multicast Routing Entry (Detail) table.

Downloaded from www.Manualslib.com manuals search engine

Web – Click IP, Multicast Routing, Multicast Routing Table. Click Detail to display additional information for any entry.



IP Multicast Routing Table (Summary)

Flags: P - Prune Up

Group Address	Source Address	Netmask	Interface	Owner	Flags	Detail
234.5.6.7	10.1.0.0	255.255.255.0	VLAN2	DVMRP	--	Detail
234.5.6.8	10.1.5.19	255.255.255.255	VLAN3	PIM-DM	--	Detail

Entry Count: 2

IP Multicast Routing Entry (Detail)

IP Multicast Routing Table
Flags: P ¡V Prune, F - Forwarding

Source Address:	10.1.0.0
Netmask:	255.255.255.0
Group Address:	234.5.6.7
Owner:	DVMRP
Upstream Interface:	VLAN 2
Upstream Router:	10.1.0.0
Downstream:	(none)

Downloaded from www.Manualslib.com manuals search engine

CLI – This example shows that multicast forwarding is enabled. The multicast routing table displays one entry for a multicast source routed by DVMRP, and another source routed via PIM.

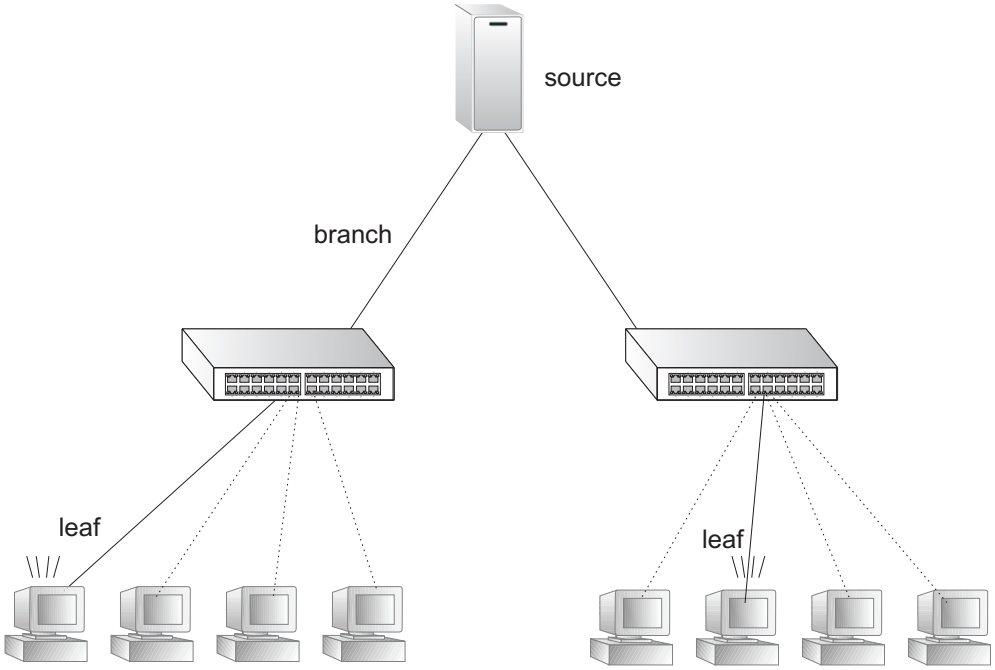
```
Console#show ip mroute3-188
IP Multicast Forwarding is enabled.

IP Multicast Routing Table

Flags:  P - Prune, F - Forwarding

(234.5.6.7, 10.1.0.0, 255.255.255.0)
Owner: DVMRP
Upstream Interface: vlan2
Upstream Router: 10.1.0.0
Downstream:


(234.5.6.8, 10.1.5.19, 255.255.255.255)
Owner: PIM-DM
Upstream Interface: vlan3
Upstream Router: 10.1.5.19
Downstream:

Console#
```

Configuring DVMRP

The Distance-Vector Multicast Routing Protocol (DVMRP) behaves somewhat similarly to RIP. A router supporting DVMRP periodically floods its attached networks to pass information about supported multicast services along to new routers and hosts. Routers that receive a DVMRP packet send a copy out to all paths (except the path back to the origin). These routers then send a prune message back to the source to stop a data stream if the router is attached to a LAN which does not want to receive traffic from a particular multicast group. However, if a host attached to this router issues an IGMP message indicating that it wants to subscribe to the concerned multicast service, this router will use DVMRP to build up a source-rooted multicast delivery tree that allows it to prevent

Downloaded from www.Manualslib.com manuals search engine

looping and determine the shortest path to the source of this multicast traffic.



When this router receives the multicast message, it checks its unicast routing table to locate the port that provides the shortest path back to the source. If that path passes through the same port on which the multicast message was received, then this router records path information for the concerned multicast group in its routing table and forwards the multicast message on to adjacent routers, except for the port through which the message arrived. This process eliminates potential loops from the tree and ensures that the shortest path (in terms of hop count) is always used.

Configuring Global DVMRP Settings

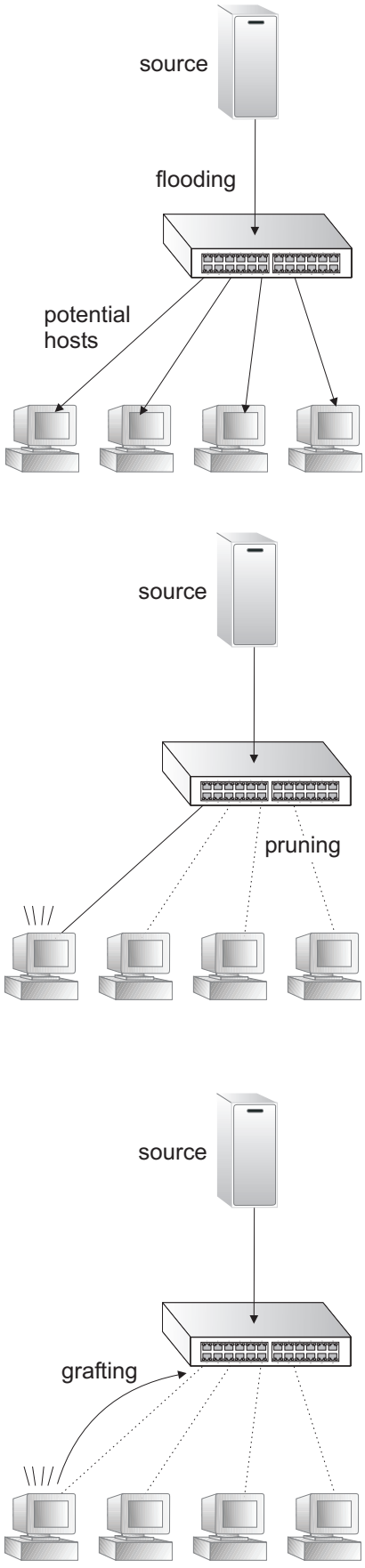
DVMRP is used to route multicast traffic to nodes which have requested a specific multicast service via IGMP. This router uses Reverse Path Forwarding (RPF) to build a shortest-path delivery tree that begins at the source and spreads out to reach group members through the network. RPF uses three different techniques to dynamically reconfigure the multicast spanning tree: broadcasting, pruning, and grafting.

Downloaded from www.Manualslib.com manuals search engine

Command Usage

Downloaded from www.Manualslib.com manuals search engine

Broadcasting periodically floods the



Downloaded from www.Manualslib.com manuals search engine

network with traffic from any active multicast server. If IGMP snooping is disabled, multicast traffic is flooded to all ports on the router. However, if IGMP snooping is enabled, then the first packet for any source group pair is flooded to all DVMRP downstream neighbors. If a packet is received through an interface that the router determines to be the shortest path back to the source (based on interface metrics), then the router forwards the packet on all interfaces except for the incoming interface.

The router will transmit a prune message back out the receiving interface (i.e., the parent interface) to its upstream neighboring router if there are no group members on its child interfaces. A prune message tells the upstream router to stop forwarding packets for a particular source-group pair for the prune lifetime.

If the router that previously sent a prune message now discovers a new group member on one of its connections, it sends a graft message to the upstream router. When an upstream router receives this message, it cancels the prune message. If necessary, graft messages are propagated back toward the source until reaching the nearest live branch in the multicast tree.

The global settings that control the prune and graft messages (i.e., prune lifetime) should be configured to the same values on all routers throughout the network to allow DVMRP to function properly. However, if you encounter problems in maintaining a multicast flow, then you may need to modify the protocol variables which control the exchange of topology information between DVMRP routers; such as the probe interval, neighbor timeout or report interval.

Command Attributes

- **DVMRP Protocol** – Enables/disables DVMRP globally. (Default: Disabled)

- **Probe Interval** – Sets the interval for sending neighbor probe messages to the multicast group address for all DVMRP routers. Probe messages are sent to neighboring DVMRP routers from which this device has received probes, and is used to verify whether or not these

Downloaded from www.Manualslib.com manuals search engine

neighbors are still active members of the multicast tree. (Range: 1-65535 seconds; Default: 10 seconds)

- **Neighbor Timeout Interval** – Sets the interval to wait for messages from a DVMRP neighbor before declaring it dead. This command is used for timing out routes, and for setting the children and leaf flags. (Range: 1-65535 seconds; Default: 35 seconds)

- **Report Interval** – Specifies how often to propagate the complete set of routing tables to other neighbor DVMRP routers. (Range: 1-65535 seconds; Default: 60 seconds)

- **Flash Update Interval** – Specifies how often to send trigger updates, which reflect changes in the network topology.

- **Prune Lifetime** – Specifies how long a prune state will remain in effect for a multicast tree. (Range: 1-65535; Default: 7200 seconds)

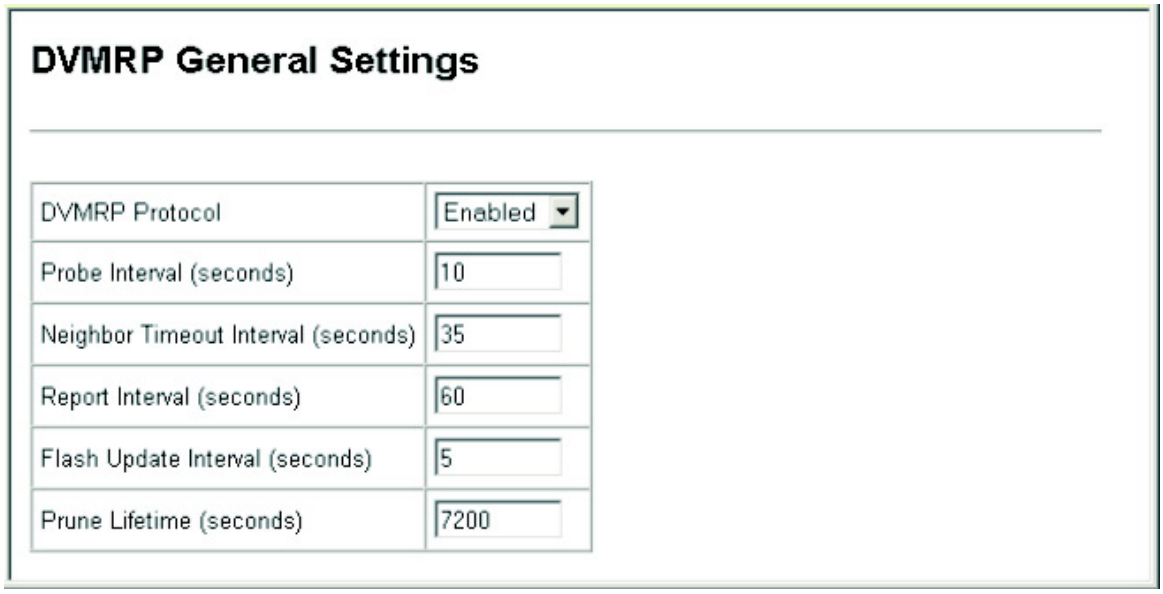
- **Default Gateway*** – Specifies the default DVMRP gateway for IP multicast traffic. (Default: none)

  - The specified interface advertises itself as a default route to neighboring DVMRP routers. It advertises the default route out through its other interfaces. Neighboring routers on the other interfaces return Poison Reverse messages for the default route back to the router. When the router receives these messages, it records all the downstream routers for the default route.
  - When multicast traffic with an unknown source address (i.e., not found in the route table) is received on the default upstream route interface, the router forwards this traffic out through the other interfaces (with known downstream routers). However, when multicast traffic with an unknown source address is received on another interface, the router drops it because only the default upstream interface can forward multicast traffic from an unknown source.

* CLI only.

Downloaded from www.Manualslib.com manuals search engine

Web – Click Routing Protocol, DVMRP, General Settings. Enable or disable DVMRP. Set the global parameters that control neighbor timeout, the exchange of routing information, or the prune lifetime, and click Apply.



CLI – This sets the global parameters for DVMRP and displays the current settings.

```
Console(config)#router dvmrp3-191
Console(config-router)#probe-interval 303-192
Console(config-router)#nbr-timeout 403-193
Console(config-router)#report-interval 903-194
Console(config-router)#flash-update-interval 103-194
Console(config-router)#prune-lifetime 50003-195
Console(config-router)#default-gateway 10.1.0.2533-196
Console(config-router)#end
Console#show router dvmrp3-199
Admin Status                    : enable
Probe Interval                  : 10
Nbr expire                      : 35
Minimum Flash Update Interval   : 5
prune lifetime                  : 7200
route report                    : 60
Default Gateway                 :
Console#
```

Configuring DVMRP Interface Settings

To fully enable DVMRP, you need to enable multicast routing globally for the router (page 3-319), enable DVMRP globally for the router

Downloaded from www.Manualslib.com manuals search engine

(page 3-324), and also enable DVMRP for each interface that will participate in multicast routing.

Command Attributes

DVMRP Interface Information

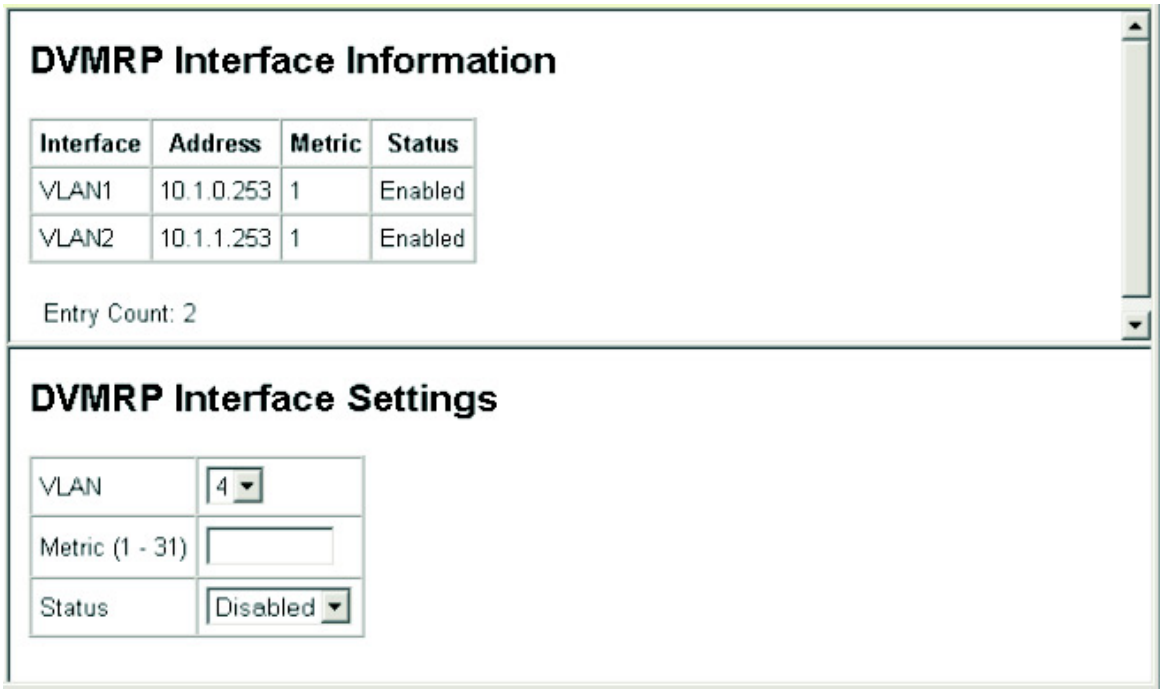
- **Interface** – VLAN interface on this router that has enabled DVMRP.
- **Address** – IP address of this VLAN interface.
- **Metric** – The metric for this interface used to calculate distance vectors.
- **Status** – Shows that DVMRP is enabled on this interface.

DVMRP Interface Settings

- **VLAN** – Selects a VLAN interface on this router.
- **Metric** – Sets the metric for this interface used to calculate distance vectors.
- **Status** – Enables or disables DVMRP.
  - If DVMRP is enabled on any interface, Layer 3 IGMP should also be enabled on the router (page 3-200).
  - If DVMRP is disabled, the interface cannot propagate IP multicast routing information. However, as long as IGMP snooping is enabled, the interface will still forward multicast traffic to downstream group members within the VLAN. But if IGMP snooping is disabled, then the interface will flood incoming multicast traffic to all ports in the attached VLAN.

Downloaded from www.Manualslib.com manuals search engine

Web – Click Routing Protocol, DVMRP, Interface Settings. Select a VLAN from the drop-down box under DVMRP Interface Settings, modify the Metric if required, set the Status to Enabled or Disabled, and click Apply.



CLI – This example enables DVMRP and sets the metric for VLAN 1.

```
Console(config)#interface vlan 13-1
Console(config-if)#ip dvmrp3-197
Console(config-if)#ip dvmrp metric 23-198
Console(config-if)#end
Console#show ip dvmrp interface3-202
Vlan 1 is up
  DVMRP is enabled
  Metric is 2

Console#
```

Displaying Neighbor Information

You can display all the neighboring DVMRP routers.

Command Attributes

- **Neighbor Address** – The IP address of the network device immediately upstream for this multicast delivery tree.

- **Interface** – The IP interface on this router that connects to the

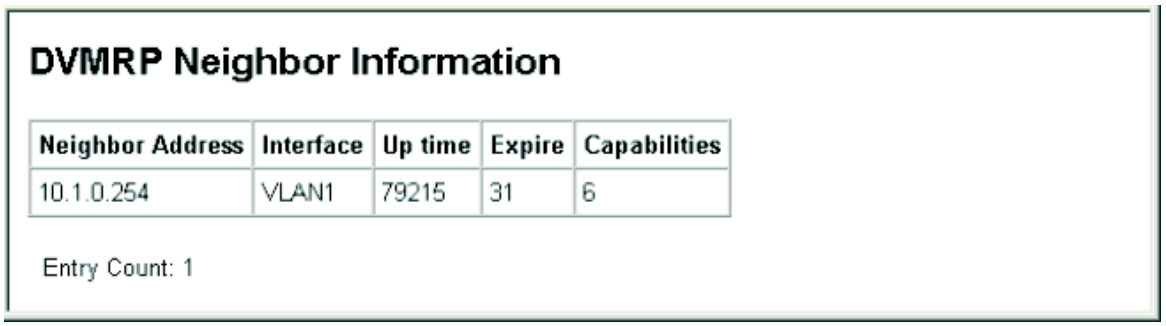
Downloaded from www.Manualslib.com manuals search engine

upstream neighbor.

- **Up time** – The time since this device last became a DVMRP neighbor to this router.
- **Expire** – The time remaining before this entry will be aged out.
- **Capabilities** – A hexadecimal value that indicates the neighbor's capabilities. Each time a probe message is received from a neighbor, the router compares the capabilities bits with the previous version for that neighbor to check for changes in neighbor capabilities. (Refer to DVMRP IETF Draft v3-10 section 3.2.1 for a detailed description of these bits). These bits are described below:

  - Leaf (bit 0) - Neighbor has only one interface with neighbors.
  - Prune (bit 1) - Neighbor supports pruning.
  - Generation ID (bit 2) - Neighbor sends its Generation ID in probe messages.
  - Mtrace (bit 3) - Neighbor can handle multicast trace requests.
  - SNMP (bit 4) - Neighbor is SNMP capable.
  - Netmask - (bit 5) - Neighbor will accept network masks appended to the prune, graft, and graft acknowledgement messages.
  - Reserved (bit 6 and 7) - Reserved for future use.

Web – Click Routing Protocol, DVMRP, Neighbor Information.



Downloaded from www.Manualslib.com manuals search engine

CLI – This example displays the only neighboring DVMRP router.

```
Console#show ip dvmrp neighbor3-201

     Address        Interface     Uptime   Expire   Capabilities
--------------- --------------- -------- -------- -------------
      10.1.0.254           vlan1    79315       32             6
Console#
```

Displaying the Routing Table

The router learns source-routed information from neighboring DVMRP routers and also advertises learned routes to its neighbors. The router merely records path information it has learned on its own or from other routers. It does not consider group membership or prune messages. Information stored in the routing table includes subnetworks from which IP multicast traffic originates, upstream routers that have sent multicast traffic in the past or have been learned through routing messages exchanged with other routers, interfaces connected to an upstream router, or outgoing interfaces that are connected to multicast hosts.

The DVMRP routing table contains multicast route information learned via DVMRP route updates, and is used to forward IP multicast traffic. The routes listed in the table do not reflect actual multicast traffic flows. For this information, you should look at the IGMP Member Port Table (page 3-199) or the IGMP Group Membership Table (page 3-205).

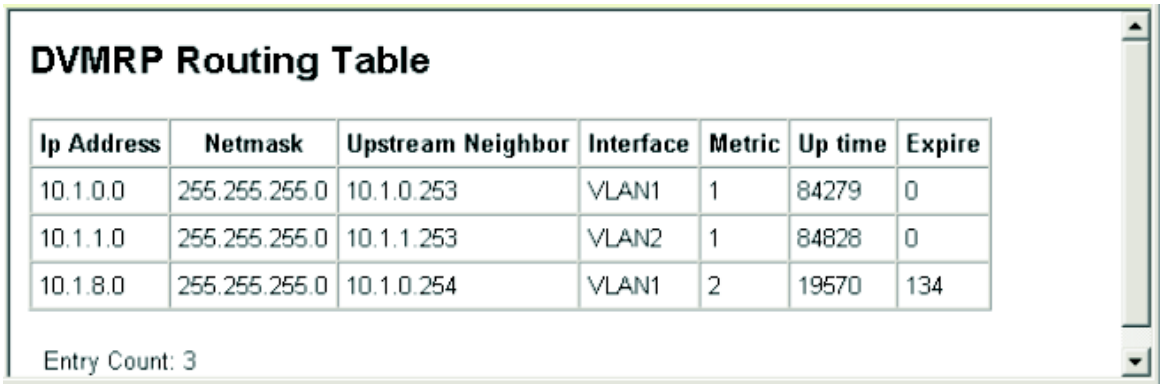
Command Attributes

- **IP Address** – IP subnetwork that contains a multicast source, an upstream router, or an outgoing interface connected to multicast hosts.
- **Netmask** – Subnet mask that is used for the source address. This mask identifies the host address bits used for routing to specific subnets.
- **Upstream Neighbor** – IP address of the network device immediately upstream for each multicast group.
- **Interface** – The IP interface on this router that connects to the upstream neighbor.
- **Metric** – The metric for this interface used to calculate distance vectors.
- **Up time** – The time elapsed since this entry was created.

Downloaded from www.Manualslib.com manuals search engine

- **Expire** – The time remaining before this entry will be aged out.

Web – Click Routing Protocol, DVMRP, DVMRP Routing Table.



DVMRP Routing Table

Ip Address	Netmask	Upstream Neighbor	Interface	Metric	Up time	Expire
10.1.0.0	255.255.255.0	10.1.0.253	VLAN1	1	84279	0
10.1.1.0	255.255.255.0	10.1.1.253	VLAN2	1	84828	0
10.1.8.0	255.255.255.0	10.1.0.254	VLAN1	2	19570	134

Entry Count: 3

CLI – This example displays known DVMRP routes.

```
Console#show ip dvmrp route3-200

    Source          Mask      Upstream_nbr   Interface Metric UpTime Expire
--------------- --------------- --------------- --------- ------ ------
------
      10.1.0.0   255.255.255.0     10.1.0.253     vlan1      1  84438      0
      10.1.1.0   255.255.255.0     10.1.1.253     vlan2      1  84987      0
      10.1.8.0   255.255.255.0     10.1.0.254     vlan1      2  19729     97
Console#
```

Configuring PIM-DM

Protocol-Independent Multicasting (PIM) provides two different modes of operation: sparse mode and dense mode. Sparse mode (SM) is designed for networks where the probability of multicast group members is low, such as the Internet. Dense mode (DM), on the other hand, is designed for networks where the probability of multicast group members is high, such as a local network.

PIM-DM is a simple multicast routing protocol that uses flood and prune to build a source-routed multicast delivery tree for each multicast source-group pair. It is simpler than DVMRP because it does not maintain it's own routing table. Instead, it uses the routing table provided by the unicast routing protocol enabled on the router interface. When the router receives a multicast packet for a source-group pair, PIM-DM checks the unicast routing table on the inbound interface to determine if this is the

Downloaded from www.Manualslib.com manuals search engine

same interface used for routing unicast packets to the multicast source network. If it is not, the router drops the packet and sends a prune message back out the source interface. If it is the same interface used by the unicast protocol, then the router forwards a copy of the packet to all the other interfaces for which is has not already received a prune message for this specific source-group pair.

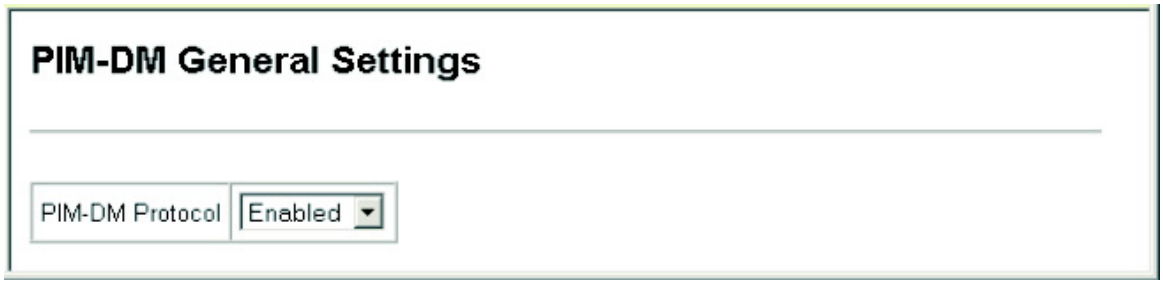
DVMRP holds the prune state for about two hours, while PIM-DM holds it for only about three minutes. This results in more flooding than encountered with DVMRP, but this the only major trade-off for the lower processing overhead and simplicity of configuration for PIM-DM.

Configuring Global PIM-DM Settings

PIM-DM is used to route multicast traffic to nodes which have requested a specific multicast service via IGMP. It uses the router's unicast routing table to determine if the interface through which a packet is received provides the shortest path back to the source. This is done on a per hop basis back toward the source of the multicast delivery tree. PIM-DM uses three different techniques to dynamically reconfigure the multicast spanning tree: broadcasting, pruning, and grafting.

To use PIM-DM, you must enable it globally for the router as described below, and for each interface that will support multicast routing as described in the next section. Also note that IGMP must be enabled to allow the router to determine the location of group members.

Web – Click Routing Protocol, PIM-DM, General Settings. Enable or disable PIM-DM globally for the router, and click Apply.



Downloaded from www.Manualslib.com manuals search engine

CLI – This example enables PIM-DM globally and displays the current status.

```
Console(config)#router pim3-203
Console#show router pim3-209
Admin Status: Enabled
Console#
```

Configuring PIM-DM Interface Settings

To fully enable PIM-DM, you need to enable multicast routing globally for the router (page 3-319), enable PIM-DM globally for the router (page 3-335), and also enable PIM-DM for each interface that will participate in multicast routing.

Command Usage

- PIM-DM functions similar to DVMRP by periodically flooding the network with traffic from any active multicast server (page 3-323). It also uses IGMP to determine the presence of multicast group members. The main difference, is that it uses the router's unicast routing table to determine if the interface through which a packet is received provides the shortest path back to the source.
- Dense-mode interfaces are subject to multicast flooding by default, and are only removed from the multicast routing table when the router determines that there are no group members or downstream routers, or when a prune message is received from a downstream router.
- The interface settings that control the prune and graft messages (i.e., prune holdtime) should be configured to the same values on all routers throughout the network to allow PIM to function properly.

Command Attributes

- **VLAN** – Selects a VLAN interface on this router.
- **PIM-DM Protocol Status** – Enables/disables PIM-DM. (Default: Disabled)
- **Hello Interval** – Sets the frequency at which PIM hello messages are

Downloaded from www.Manualslib.com manuals search engine

transmitted. Hello messages are sent to neighboring PIM routers from which this device has received probes, and are used to verify whether or not these neighbors are still active members of the multicast tree. (Range: 1-65535 seconds; Default: 30)

- **Hello Holdtime** – Sets the interval to wait for hello messages from a neighboring PIM router before declaring it dead. Note that the hello holdtime should be 3.5 times the value of Hello Interval. (Range: 1-65535 seconds; Default: 105)

- **Trigger Hello Interval** – Configures the maximum time before transmitting a triggered PIM hello message after the router is rebooted or PIM is enabled on an interface. (Range: 1-65535 seconds; Default: 5)

  - When a router first starts or PIM is enabled on an interface, the hello-interval is set to random value between 0 and the Trigger Hello Interval. This prevents synchronization of Hello messages on multi-access links if multiple routers are powered on simultaneously.
  - Also, if a Hello message is received from a new neighbor, the receiving router will send its own Hello message after a random delay between 0 and the Trigger Hello Interval.

- **Prune Holdtime** – Configures of the hold time for the prune state. The multicast interface that first receives a multicast stream from a particular source forwards this traffic to all other PIM interfaces on the router. If there are no requesting groups on that interface, the leaf node sends a prune message upstream and enters a prune state for this multicast stream. The prune state is maintained until the prune holdtime timer expires or a graft message is received for the forwarding entry. (Range: 1-65535 seconds; Default: 210)

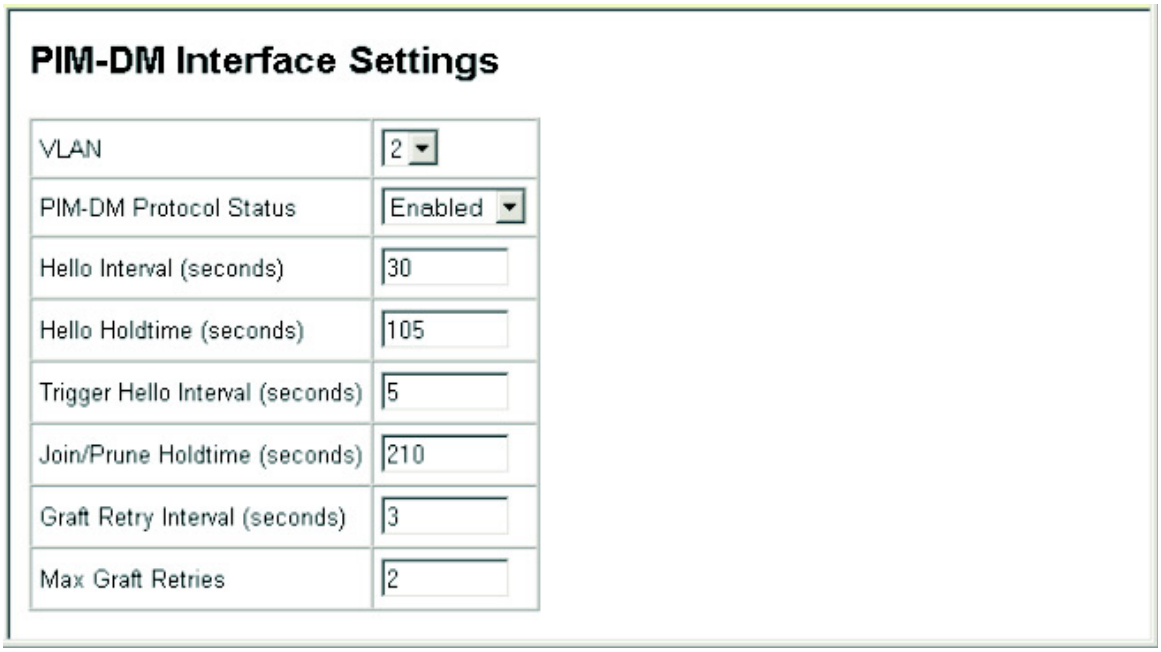
- **Graft Retry Interval** – Configures the time to wait for a graft acknowledgement before resending a graft. A graft message is sent by a router to cancel a prune state. When a router receives a graft message, it must respond with an graft acknowledgement message. If this

Downloaded from www.Manualslib.com manuals search engine

acknowledgement message is lost, the router that sent the graft message will resend it a maximum number of times as defined by Max Graft Retries. (Range: 1-65535 seconds; Default: 3)

- **Max Graft Retries** – Configures the maximum number of times to resend a graft message if it has not been acknowledged. (Range: 1-65535; Default: 2)

Web – Click Routing Protocol, PIM-DM, Interface Settings. Select a VLAN, enable or disable PIM-DM for the selected interface, modify any of the protocol parameters as required, and click Apply.



Downloaded from www.Manualslib.com manuals search engine

CLI – This example sets the PIM-DM protocol parameters for VLAN 2, and displays the current settings.

```
Console(config)#interface vlan 23-57
Console(config-if)#ip pim dense-mode3-204
Console(config-if)#ip pim hello-interval 603-205
Console(config-if)#ip pim hello-holdtime 2103-206
Console(config-if)#ip pim trigger-hello-interval 103-206
Console(config-if)#ip pim join-prune-holdtime 603-207
Console(config-if)#ip pim graft-retry-interval 93-208
Console(config-if)#ip pim max-graft-retries 53-209
Console(config-if)#end
Console#show ip pim interface 23-210
Vlan 2 is up
 PIM is enabled, mode is Dense.
 Internet address is 10.1.1.253.
 Hello time interval is 60 sec, trigger hello time interval is 10 sec.
 Hello holdtime is 210 sec.
 Join/Prune holdtime is 60 sec.
 Graft retry interval is 9 sec, max graft retries is 5.
 DR Internet address is 10.1.1.253, neighbor count is 0.

Console#
```

Displaying Interface Information

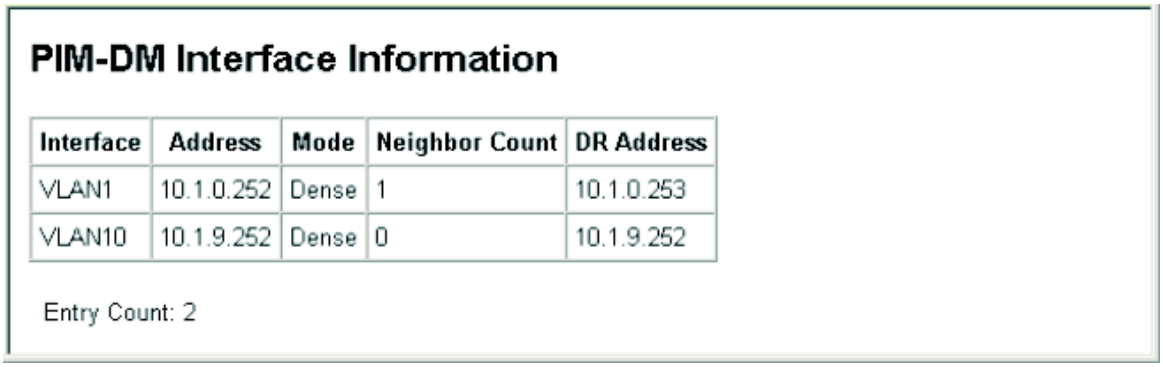
You can display a summary of the current interface status for PIM-DM, including the number of neighboring PIM routers, and the address of the designated PIM router.

Command Attributes

- **Interface** – A VLAN interface on this router.
- **Address** – The IP address for this interface.
- **Mode** – The PIM mode in use. (This router only supports Dense Mode at this time.)
- **Neighbor Count** – The number of PIM neighbors detected on this interface.
- **DR Address** – The designated PIM router for this interface.

Downloaded from www.Manualslib.com manuals search engine

Web – Click Routing Protocol, PIM-DM, Interface Information.



PIM-DM Interface Information

Interface	Address	Mode	Neighbor Count	DR Address
VLAN1	10.1.0.252	Dense	1	10.1.0.253
VLAN10	10.1.9.252	Dense	0	10.1.9.252

Entry Count: 2

CLI – This example shows the PIM-DM interface summary for VLAN 1.

```
Console#show ip pim interface 13-210
Vlan 1 is up
 PIM is enabled, mode is Dense.
 Internet address is 10.1.0.253.
 Hello time interval is 30 sec, trigger hello time interval is 5 sec.
 Hello holdtime is 105 sec.
 Join/Prune holdtime is 210 sec.
 Graft retry interval is 3 sec, max graft retries is 2.
 DR Internet address is 10.1.0.253, neighbor count is 1.

Console#
```

Displaying Neighbor Information

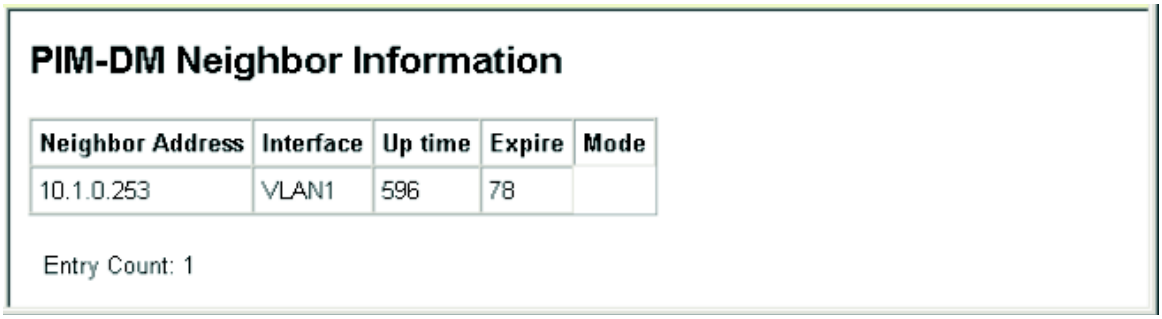
You can display all the neighboring PIM-DM routers.

Command Attributes

- **Neighbor Address** – IP address of the next-hop router.
- **Interface** – VLAN that is attached to this neighbor.
- **Up time** – The duration this entry has been active.
- **Expire** – The time before this entry will be removed.
- **Mode** – PIM mode used on this interface. (Only Dense Mode is supported.)

Downloaded from www.Manualslib.com manuals search engine

Web – Click Routing Protocol, PIM-DM, Neighbor Information.



PIM-DM Neighbor Information

Neighbor Address	Interface	Up time	Expire	Mode
10.1.0.253	VLAN1	596	78	

Entry Count: 1

CLI – This example displays the only neighboring PIM-DM router.

```
Console#show ip pim neighbor3-210
    Address      VLAN Interface   Uptime   Expire   Mode
--------------- ---------------- -------- -------- -------

     10.1.0.253               1      613       91   Dense
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 4
COMMAND LINE INTERFACE

This chapter describes how to use the Command Line Interface (CLI).

Using the Command Line Interface

Accessing the CLI

When accessing the management interface for the switch over a direct connection to the server's console port, or via a Telnet connection, the switch can be managed by entering command keywords and parameters at the prompt. Using the switch's command-line interface (CLI) is very similar to entering commands on a UNIX system.

Console Connection

To access the switch through the console port, perform these steps:

1. At the console prompt, enter the user name and password. (The default user names are "admin" and "guest" with corresponding passwords of "admin" and "guest.") When the administrator user name and password is entered, the CLI displays the "Console#" prompt and enters privileged access mode (i.e., Privileged Exec). But when the guest user name and password is entered, the CLI displays the "Console>" prompt and enters normal access mode (i.e., Normal Exec).

2. Enter the necessary commands to complete your desired tasks.

3. When finished, exit the session with the "quit" or "exit" command.

Downloaded from www.Manualslib.com manuals search engine

After connecting to the system through the console port, the login screen displays:

```
User Access Verification

Username: admin
Password:

     CLI session with the SMC8612XL3 is opened.
      To end the CLI session, enter [Exit].

Console#
```

Telnet Connection

Telnet operates over the IP transport protocol. In this environment, your management station and any network device you want to manage over the network must have a valid IP address. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. Each address consists of a network portion and host portion. For example, the IP address assigned to this switch, 10.1.0.1, consists of a network portion (10.1.0) and a host portion (1).

Note: The IP address for this switch is unassigned by default.

To access the switch through a Telnet session, you must first set the IP address for the switch, and set the default gateway if you are managing the switch from a different IP subnet. For example,

```
Console(config)#interface vlan 1
Console(config-if)#ip address 10.1.0.254 255.255.255.0
Console(config-if)#exit
Console(config)#ip default-gateway 10.1.0.254
```

If your corporate network is connected to another network outside your office or to the Internet, you need to apply for a registered IP address. However, if you are attached to an isolated network, then you can use any IP address that matches the network segment to which you are attached.

Downloaded from www.Manualslib.com manuals search engine

After you configure the switch with an IP address, you can open a Telnet session by performing these steps:

1. From the remote host, enter the Telnet command and the IP address of the device you want to access.

2. At the prompt, enter the user name and system password. The CLI will display the "Vty-0#" prompt for the administrator to show that you are using privileged access mode (i.e., Privileged Exec), or "Vty-0>" for the guest to show that you are using normal access mode (i.e., Normal Exec).

3. Enter the necessary commands to complete your desired tasks.

4. When finished, exit the session with the "quit" or "exit" command.

After entering the Telnet command, the login screen displays:

```
Username: admin
Password:

     CLI session with the SMC8612XL3 is opened.
      To end the CLI session, enter [Exit].

Vty-0#
```

Note: You can open up to four sessions to the device via Telnet.

Downloaded from www.Manualslib.com manuals search engine

Entering Commands

This section describes how to enter CLI commands.

Keywords and Arguments

A CLI command is a series of keywords and arguments. Keywords identify a command, and arguments specify configuration parameters. For example, in the command "show interfaces status ethernet 1/5," **show interfaces** and **status** are keywords, **ethernet** is an argument that specifies the interface type, and **1/5** specifies the unit/port.

You can enter commands as follows:

- To enter a simple command, enter the command keyword.
- To enter multiple commands, enter each command in the required order. For example, to enable Privileged Exec command mode, and display the startup configuration, enter:

```
Console>enable
Console#show startup-config
```

- To enter commands that require parameters, enter the required parameters after the command keyword. For example, to set a password for the administrator, enter:

```
Console(config)#username admin password 0 smith
```

Minimum Abbreviation

The CLI will accept a minimum number of characters that uniquely identify a command. For example, the command "configure" can be entered as **con**. If an entry is ambiguous, the system will prompt for further input.

Downloaded from www.Manualslib.com manuals search engine

Command Completion

If you terminate input with a Tab key, the CLI will print the remaining characters of a partial keyword up to the point of ambiguity. In the "logging history" example, typing **log** followed by a tab will result in printing the command up to "**logging**."

Getting Help on Commands

You can display a brief description of the help system by entering the **help** command. You can also display command syntax by using the "?" character to list keywords or parameters.

Downloaded from www.Manualslib.com manuals search engine

Showing Commands

If you enter a "?" at the command prompt, the system will display the first level of keywords for the current command class (Normal Exec or Privileged Exec) or configuration class (Global, ACL, DHCP, Interface, Line, VLAN Database, or MSTP). You can also display a list of valid keywords for a specific command. For example, the command "**show ?**" displays a list of possible show commands:

```
Console#show ?
  access-group        Access groups
  access-list         Access lists
  arp                 Information of arp cache
  bridge-ext          Bridge extend information
  calendar            Date information
  dns                 DNS information
  dot1x               Show 802.1x content
  garp                Garp property
  gvrp                Show GVRP information of interface
  history             Information of history
  hosts               Host information
  interfaces          Information of interfaces
  ip                  IP information
  line                TTY line information
  logging             Show the contents of logging buffers
  mac                 MAC access lists
  mac-address-table   Set configuration of the address table
  management          Show management ip filter
  map                 Map priority
  port                Characteristics of the port
  protocol-vlan       Protocol-vlan information
  public-key          Show information of public key
  pvlan               Information of private VLAN
  queue               Information of priority queue
  radius-server       RADIUS server information
  rip                 Rip
  router              Router
  running-config      The system configuration of running
  snmp                SNMP statistics
  sntp                Sntp
  spanning-tree       Specify spanning-tree
  ssh                 Secure shell
  startup-config      The system configuration of starting up
  system              Information of system
  tacacs-server       Login by tacacs server
  users               Display information about terminal lines
  version             System hardware and software status
  vlan                Switch VLAN Virtual Interface
Console#show
```


Downloaded from www.Manualslib.com manuals search engine

The command "**show interfaces ?**" will display the following information:

```
Console#show interfaces ?
  counters       Information of interfaces counters
  protocol-vlan  Protocol-vlan information
  status         Information of interfaces status
  switchport     Information of interfaces switchport
Console#
```

Partial Keyword Lookup

If you terminate a partial keyword with a question mark, alternatives that match the initial letters are provided. (Remember not to leave a space between the command and question mark.) For example "**s?**" shows all the keywords starting with "s."

```
Console#show s?
snmp           sntp           spanning-tree   ssh           startup-config
system
```

Negating the Effect of Commands

For many configuration commands you can enter the prefix keyword "**no**" to cancel the effect of a command or reset the configuration to the default value. For example, the **logging** command will log system messages to a host server. To disable logging, specify the **no logging** command. This guide describes the negation effect for all applicable commands.

Using Command History

The CLI maintains a history of commands that have been entered. You can scroll back through the history of commands by pressing the up arrow key. Any command displayed in the history list can be executed again, or first modified and then executed.

Using the **show history** command displays a longer list of recently executed commands.

Downloaded from www.Manualslib.com manuals search engine

Understanding Command Modes

The command set is divided into Exec and Configuration classes. Exec commands generally display information on system status or clear statistical counters. Configuration commands, on the other hand, modify interface parameters or enable certain switching functions. These classes are further divided into different modes. Available commands depend on the selected mode. You can always enter a question mark "**?**" at the prompt to display a list of the commands available for the current mode. The command classes and associated modes are displayed in the following table:

Class	Mode	
Exec	Normal Privileged	
Configuration	Global*	Access Control List DHCP Interface Line Multiple Spanning Tree Router VLAN Database

* You must be in Privileged Exec mode to access the Global configuration mode.

You must be in Global Configuration mode to access any of the other configuration modes.

Exec Commands

When you open a new console session on the switch with the user name and password "guest," the system enters the Normal Exec command mode (or guest mode), displaying the "Console>" command prompt. Only a limited number of the commands are available in this mode. You can access all commands only from the Privileged Exec command mode (or administrator mode). To access Privilege Exec mode, open a new

Downloaded from www.Manualslib.com manuals search engine

console session with the user name and password "admin." The system will now display the "Console#" command prompt. You can also enter Privileged Exec mode from within Normal Exec mode, by entering the **enable** command, followed by the privileged level password "super" (page 3-37).

To enter Privileged Exec mode, enter the following user names and passwords:

```
Username: admin
Password: [admin login password]

     CLI session with the SMC8612XL3 is opened.
      To end the CLI session, enter [Exit].

Console#
```

```
Username: guest
Password: [guest login password]

     CLI session with the SMC8612XL3 is opened.
      To end the CLI session, enter [Exit].

Console#enable
Password: [privileged level password]
Console#
```

Configuration Commands

Configuration commands are privileged level commands used to modify switch settings. These commands modify the running configuration only and are not saved when the switch is rebooted. To store the running configuration in non-volatile storage, use the **copy running-config startup-config** command.

The configuration commands are organized into different modes:

- Global Configuration - These commands modify the system level configuration, and include commands such as **hostname** and **snmp-server community**.
- Access Control List Configuration - These commands are used for

Downloaded from www.Manualslib.com manuals search engine

packet filtering.

- DHCP Configuration - These commands are used to configure the DHCP server.
- Interface Configuration - These commands modify the port configuration such as **speed-duplex** and **negotiation**.
- Line Configuration - These commands modify the console port and Telnet configuration, and include command such as **parity** and **databits**.
- Router Configuration - These commands configure global settings for unicast and multicast routing protocols.
- VLAN Configuration - Includes the command to create VLAN groups.
- Multiple Spanning Tree Configuration - These commands configure settings for the selected multiple spanning tree instance.

To enter the Global Configuration mode, enter the command **configure** in Privileged Exec mode. The system prompt will change to "Console(config)#" which gives you access privilege to all Global Configuration commands.

```
Console#configure
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

To enter the other modes, at the configuration prompt type one of the following commands. Use the **exit** or **end** command to return to the Privileged Exec mode.

Mode	Command	Prompt	Page
Line	line {console | vty}	Console(config-line)#	3-15
Access Control List	access-list ip standard access-list ip extended access-list ip mask-precedence access-list mac access-list mac mask-precedence	Console(config-std-acl) Console(config-ext-acl) Console(config-ip-mask-acl) Console(config-mac-acl) Console(config-mac-mask-acl)	3-113
DHCP	ip dhcp pool	Console(config-dhcp)	3-155
Interface	interface {ethernet *port* | port-channel *id*| vlan *id*}	Console(config-if)#	3-1
VLAN	vlan database	Console(config-vlan)	3-54
MSTP	spanning-tree mst-configuration	Console(config-mstp)#	4-168
Router	router {rip | ospf | dvmrp | pim}	Console(config-router)	3-132 3-146 3-191 3-203

For example, you can use the following commands to enter interface configuration mode, and then return to Privileged Exec mode

```
Console(config)#interface ethernet 1/5
.
.
.
Console(config-if)#exit
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

Command Line Processing

Commands are not case sensitive. You can abbreviate commands and parameters as long as they contain enough letters to differentiate them from any other currently available commands or parameters. You can use the Tab key to complete partial commands, or enter a partial command followed by the "?" character to display a list of possible matches. You can also use the following editing keystrokes for command-line processing:

Keystroke	Function
Ctrl-A	Shifts cursor to start of command line.
Ctrl-B	Shifts cursor to the left one character.
Ctrl-C	Terminates the current task and displays the command prompt.
Ctrl-E	Shifts cursor to end of command line.
Ctrl-F	Shifts cursor to the right one character.
Ctrl-K	Deletes all characters from the cursor to the end of the line.
Ctrl-L	Repeats current command line on a new line.
Ctrl-N	Enters the next command line in the history buffer.
Ctrl-P	Enters the last command.
Ctrl-R	Repeats current command line on a new line.
Ctrl-U	Deletes from the cursor to the beginning of the line.
Ctrl-W	Deletes the last word typed.
Esc-B	Moves the cursor back one word.
Esc-D	Deletes from the cursor to the end of the word.
Esc-F	Moves the cursor forward one word.
Delete key or backspace key	Erases a mistake when entering a command.

Downloaded from www.Manualslib.com manuals search engine

Command Groups

The system commands can be broken down into the functional groups shown below.

Command Group	Description	Page
Line	Sets communication parameters for the serial port and Telnet, including baud rate and console time-out	3-15
General	Basic commands for entering privileged access mode, restarting the system, or quitting the CLI	3-27
System Management	Controls system logs, system passwords, user name, browser management options, and a variety of other system information	3-33
Flash/File	Manages code image or switch configuration files	3-85
Authentication	Configures logon access using local or remote authentication; also configures port security and IEEE 802.1x port access control	3-92
Access Control List	Provides filtering for IP frames (based on address, protocol, TCP/UDP port number or TCP control code) or non-IP frames (based on MAC address or Ethernet type)	3-113
SNMP	Activates authentication failure traps; configures community access strings, and trap managers; also configures IP address filtering	3-147
DHCP	Configures DHCP client, relay and server functions	3-155
DNS	Configures DNS services.	3-176
Interface	Configures the connection parameters for all Ethernet ports, aggregated links, and VLANs	3-1
Mirror Port	Mirrors data to another port for analysis without affecting the data passing through or the performance of the monitored port	3-16
Rate Limiting	Controls the maximum rate for traffic transmitted or received on a port	3-18
Link Aggregation	Statically groups multiple ports into a single logical trunk; configures Link Aggregation Control Protocol for port trunks	3-20

Downloaded from www.Manualslib.com manuals search engine

Command Group	Description	Page
Address Table	Configures the address table for filtering specified addresses, displays current entries, clears the table, or sets the aging time	3-33
Spanning Tree	Configures Spanning Tree settings for the switch	3-38
VLANs	Configures VLAN settings, and defines port membership for VLAN groups; also enables or configures private VLANs and protocol VLANs	3-54
GVRP and Bridge Extension	Configures GVRP settings that permit automatic VLAN learning; shows the configuration for the bridge extension MIB	3-71
Priority	Sets port priority for untagged frames, selects strict priority or weighted round robin, relative weight for each priority queue, also sets priority for TCP traffic types, IP precedence, and DSCP	3-77
Multicast Filtering	Configures IGMP multicast filtering, query parameters, and specifies ports attached to a multicast router	3-95
IP Interface	Configures IP address for the switch interfaces; also configures ARP parameters and static entries	3-116
IP Routing	Configures static and dynamic unicast routing	3-126
Multicast Routing	Configures multicast routing protocols DVMRP and PIM-DM	3-184
Router Redundancy	Configures router redundancy to create primary and backup routers	3-211

Downloaded from www.Manualslib.com manuals search engine

The access mode shown in the following tables is indicated by these abbreviations:

NE (Normal Exec)
PE (Privileged Exec)
GC (Global Configuration)
LC (Line Configuration)
IC (Interface Configuration)
VC (VLAN Database Configuration)
MST (Multiple Spanning Tree)
ACL (Access Control List Configuration)
DC (DHCP Server Configuration)
RC (Router Configuration)

Line Commands

You can access the onboard configuration program by attaching a VT100 compatible device to the server's serial port. These commands are used to set communication parameters for the serial port or Telnet (i.e., a virtual terminal).

Command	Function	Mode	Page
line	Identifies a specific line for configuration and starts the line configuration mode	GC	3-16
login	Enables password checking at login	LC	3-17
password	Specifies a password on a line	LC	3-18
exec-timeout	Sets the interval that the command interpreter waits until user input is detected	LC	3-19
password-thresh	Sets the password intrusion threshold, which limits the number of failed logon attempts	LC	3-20
silent-time*	Sets the amount of time the management console is inaccessible after the number of unsuccessful logon attempts exceeds the threshold set by the **password-thresh** command	LC	3-21
databits*	Sets the number of data bits per character that are interpreted and generated by hardware	LC	3-22
parity*	Defines the generation of a parity bit	LC	3-23
speed*	Sets the terminal baud rate	LC	3-24
stopbits*	Sets the number of the stop bits transmitted per byte	LC	3-24

* These commands only apply to the serial port.

Downloaded from www.Manualslib.com manuals search engine

Command	Function	Mode	Page
disconnect	Terminates a line connection	PE	3-25
show line	Displays a terminal line's parameters	NE, PE	3-26

* These commands only apply to the serial port.

line

This command identifies a specific line for configuration, and to process subsequent line configuration commands.

Syntax

line {**console** | **vty**}

- **console** - Console terminal line.
- **vty** - Virtual terminal for remote console access (i.e., Telnet).

Default Setting

There is no default line.

Command Mode

Global Configuration

Command Usage

Telnet is considered a virtual terminal connection and will be shown as "Vty" in screen displays such as **show users**. However, the serial communication parameters (e.g., databits) do not affect Telnet connections.

Example

To enter console line mode, enter the following command:

```
Console(config)#line console
Console(config-line)#
```


Downloaded from www.Manualslib.com manuals search engine

Related Commands

show line (3-26)
show users (3-83)

login

This command enables password checking at login. Use the **no** form to disable password checking and allow connections without a password.

Syntax

login [**local**]
no login

local - Selects local password checking. Authentication is based on the user name specified with the **username** command.

Default Setting

login local

Command Mode

Line Configuration

Command Usage

- There are three authentication modes provided by the switch itself at login:
  - **login** selects authentication by a single global password as specified by the **password** line configuration command. When using this method, the management interface starts in Normal Exec (NE) mode.
  - **login local** selects authentication via the user name and password specified by the **username** command (i.e., default setting). When using this method, the management interface starts in Normal Exec (NE) or Privileged Exec (PE) mode, depending on the user's privilege level (0 or 15 respectively).
  - **no login** selects no authentication. When using this method, the management interface starts in Normal Exec (NE) mode.

Downloaded from www.Manualslib.com manuals search engine

- This command controls login authentication via the switch itself. To configure user names and passwords for remote authentication servers, you must use the RADIUS or TACACS software installed on those servers.

Example

```
Console(config-line)#login local
Console(config-line)#
```

Related Commands

username (3-35)
password (3-18)

password

This command specifies the password for a line. Use the **no** form to remove the password.

Syntax

password {**0** | **7**} *password*
no password

- {**0** | **7**} - 0 means plain password, 7 means encrypted password
- *password* - Character string that specifies the line password. (Maximum length: 8 characters plain text, 32 encrypted, case sensitive)

Default Setting

No password is specified.

Command Mode

Line Configuration

Command Usage

- When a connection is started on a line with password protection, the system prompts for the password. If you enter the correct password, the system shows a prompt. You can use the **password-thresh** command to set the number of times a user can enter an incorrect

Downloaded from www.Manualslib.com manuals search engine

password before the system terminates the line connection and returns the terminal to the idle state.

- The encrypted password is required for compatibility with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from a TFTP server. There is no need for you to manually configure encrypted passwords.

Example

```
Console(config-line)#password 0 secret
Console(config-line)#
```

Related Commands

login (3-17)
password-thresh (3-20)

exec-timeout

This command sets the interval that the system waits until user input is detected. Use the **no** form to restore the default.

Syntax

exec-timeout [*seconds*]
no exec-timeout

seconds - Integer that specifies the number of seconds. (Range: 0 - 65535 seconds; 0: no timeout)

Default Setting

CLI: No timeout
Telnet: 10 minutes

Command Mode

Line Configuration

Command Usage

- If user input is detected within the timeout interval, the session is kept open; otherwise the session is terminated.

Downloaded from www.Manualslib.com manuals search engine

- This command applies to both the local console and Telnet connections.
- The timeout for Telnet cannot be disabled.

Example

To set the timeout to two minutes, enter this command:

```
Console(config-line)#exec-timeout 120
Console(config-line)#
```

password-thresh

This command sets the password intrusion threshold which limits the number of failed logon attempts. Use the **no** form to remove the threshold value.

Syntax

password-thresh [*threshold*]
no password-thresh

threshold - The number of allowed password attempts. (Range: 1-120; 0: no threshold)

Default Setting

The default value is three attempts.

Command Mode

Line Configuration

Command Usage

- When the logon attempt threshold is reached, the system interface becomes silent for a specified amount of time before allowing the next logon attempt. (Use the **silent-time** command to set this interval.) When this threshold is reached for Telnet, the Telnet logon interface shuts down.
- This command applies to both the local console and Telnet connections.

Downloaded from www.Manualslib.com manuals search engine

Example

To set the password threshold to five attempts, enter this command:

```
Console(config-line)#password-thresh 5
Console(config-line)#
```

Related Commands

silent-time (3-21)

silent-time

This command sets the amount of time the management console is inaccessible after the number of unsuccessful logon attempts exceeds the threshold set by the **password-thresh** command. Use the **no** form to remove the silent time value.

Syntax

silent-time [*seconds*]
no silent-time

seconds - The number of seconds to disable console response. (Range: 0-65535; 0: no silent-time)

Default Setting

The default value is no silent-time.

Command Mode

Line Configuration

Example

To set the silent time to 60 seconds, enter this command:

```
Console(config-line)#silent-time 60
Console(config-line)#
```

Related Commands

password-thresh (3-20)

Downloaded from www.Manualslib.com manuals search engine

databits

This command sets the number of data bits per character that are interpreted and generated by the console port. Use the **no** form to restore the default value.

Syntax

databits {**7** | **8**}
no databits

- 7 - Seven data bits per character.
- 8 - Eight data bits per character.

Default Setting

8 data bits per character

Command Mode

Line Configuration

Command Usage

The **databits** command can be used to mask the high bit on input from devices that generate 7 data bits with parity. If parity is being generated, specify 7 data bits per character. If no parity is required, specify 8 data bits per character.

Example

To specify 7 data bits, enter this command:

```
Console(config-line)#databits 7
Console(config-line)#
```

Related Commands

parity (3-23)

Downloaded from www.Manualslib.com manuals search engine

parity

This command defines the generation of a parity bit. Use the **no** form to restore the default setting.

Syntax

parity {**none** | **even** | **odd**}
no parity

- **none** - No parity
- **even** - Even parity
- **odd** - Odd parity

Default Setting

No parity

Command Mode

Line Configuration

Command Usage

Communication protocols provided by devices such as terminals and modems often require a specific parity bit setting.

Example

To specify no parity, enter this command:

```
Console(config-line)#parity none
Console(config-line)#
```


Downloaded from www.Manualslib.com manuals search engine

speed

This command sets the terminal line's baud rate. This command sets both the transmit (to terminal) and receive (from terminal) speeds. Use the **no** form to restore the default setting.

Syntax

speed *bps*
no speed

bps - Baud rate in bits per second.
(Options: 9600, 19200, 38400, 57600, 115200 bps, or auto)

Default Setting

auto

Command Mode

Line Configuration

Command Usage

Set the speed to match the baud rate of the device connected to the serial port. Some baud rates available on devices connected to the port might not be supported. The system indicates if the speed you selected is not supported. If you select the "auto" option, the switch will automatically detect the baud rate configured on the attached terminal, and adjust the speed accordingly.

Example

To specify 57600 bps, enter this command:

```
Console(config-line)#speed 57600
Console(config-line)#
```

stopbits

This command sets the number of the stop bits transmitted per byte. Use the **no** form to restore the default setting.

Downloaded from www.Manualslib.com manuals search engine

Syntax

stopbits {**1** | **2**}

- 1 - One stop bit
- 2 - Two stop bits

Default Setting

1 stop bit

Command Mode

Line Configuration

Example

To specify 2 stop bits, enter this command:

```
Console(config-line)#stopbits 2
Console(config-line)#
```

disconnect

Use this command to terminate an SSH, Telnet, or console connection.

Syntax

disconnect *session-id*

session-id – The session identifier for an SSH, Telnet or console connection. (Range: 0-4)

Command Mode

Privileged Exec

Command Usage

Specifying session identifier "0" will disconnect the console connection. Specifying any other identifiers for an active session will disconnect an SSH or Telnet connection.

Example

```
Console#disconnect 1
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Related Commands

show ssh (3-55)
show users (3-83)

show line

This command displays the terminal line's parameters.

Syntax

show line [**console** | **vty**]

- **console** - Console terminal line.
- **vty** - Virtual terminal for remote console access (i.e., Telnet).

Default Setting

Shows all lines

Command Mode

Normal Exec, Privileged Exec

Example

To show all lines, enter this command:

```
Console#show line
 Console configuration:
  Password threshold: 3 times
  Interactive timeout: Disabled
  Silent time: Disabled
  Baudrate: 9600
  Databits: 8
  Parity: none
  Stopbits: 1
Vty configuration:
  Password threshold: 3 times
  Interactive timeout: 65535
```


Downloaded from www.Manualslib.com manuals search engine

General Commands

Command	Function	Mode	Page
enable	Activates privileged mode	NE	3-27
disable	Returns to normal mode from privileged mode	PE	3-28
configure	Activates global configuration mode	PE	3-29
show history	Shows the command history buffer	NE, PE	3-29
reload	Restarts the system	PE	3-30
end	Returns to Privileged Exec mode	any config. mode	3-31
exit	Returns to the previous configuration mode, or exits the CLI	any	3-32
quit	Exits a CLI session	NE, PE	3-32
help	Shows how to use help	any	NA
?	Shows options for command completion (context sensitive)	any	NA

enable

This command activates Privileged Exec mode. In privileged mode, additional commands are available, and certain commands display additional information. See "Understanding Command Modes" on page 4-8.

Syntax

enable [*level*]

level - Privilege level to log into the device.

The device has two predefined privilege levels: 0: Normal Exec, 15: Privileged Exec. Enter level 15 to access Privileged Exec mode.

Default Setting

Level 15

Downloaded from www.Manualslib.com manuals search engine

Command Mode

Normal Exec

Command Usage

- "super" is the default password required to change the command mode from Normal Exec to Privileged Exec. (To set this password, see the **enable password** command on page 3-37.)
- The "#" character is appended to the end of the prompt to indicate that the system is in privileged access mode.

Example

```
Console>enable
Password: [privileged level password]
Console#
```

Related Commands

disable (3-28)
enable password (3-37)

disable

This command returns to Normal Exec mode from privileged mode. In normal access mode, you can only display basic information on the switch's configuration or Ethernet statistics. To gain access to all commands, you must use the privileged mode. See "Understanding Command Modes" on page 4-8.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

The ">" character is appended to the end of the prompt to indicate that the system is in normal access mode.

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console#disable
Console>
```

Related Commands

enable (3-27)

configure

This command activates Global Configuration mode. You must enter this mode to modify any settings on the switch. You must also enter Global Configuration mode prior to enabling some of the other configuration modes, including Interface Configuration, Line Configuration, VLAN Database Configuration, and Multiple Spanning Tree Configuration. See "Understanding Command Modes" on page 4-8.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#configure
Console(config)#
```

Related Commands

end (3-31)

show history

This command shows the contents of the command history buffer.

Default Setting

None

Downloaded from www.Manualslib.com manuals search engine

Command Mode

Normal Exec, Privileged Exec

Command Usage

The history buffer size is fixed at 10 Execution commands and 10 Configuration commands.

Example

In this example, the show history command lists the contents of the command history buffer:

```
Console#show history
Execution command history:
 2 config
 1 show history

Configuration command history:
 4 interface vlan 1
 3 exit
 2 interface vlan 1
 1 end

Console#
```

The **!** command repeats commands from the Execution command history buffer when you are in Normal Exec or Privileged Exec Mode, and commands from the Configuration command history buffer when you are in any of the configuration modes. In this example, the **!2** command repeats the second command in the Execution history buffer (**config**).

```
Console#!2
Console#config
Console(config)#
```

reload

This command restarts the system.

Note: When the system is restarted, it will always run the Power-On Self-Test. It will also retain all configuration information stored in non-volatile memory by the **copy running-config startup-config**

Downloaded from www.Manualslib.com manuals search engine

command.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

This command resets the entire system.

Example

This example shows how to reset the switch:

```
Console#reload
System will be restarted, continue <y/n>? y
```

end

This command returns to Privileged Exec mode.

Default Setting

None

Command Mode

Global Configuration, Interface Configuration, Line Configuration, VLAN Database Configuration, and Multiple Spanning Tree Configuration.

Example

This example shows how to return to the Privileged Exec mode from the Interface Configuration mode:

```
Console(config-if)#end
Console#
```


Downloaded from www.Manualslib.com manuals search engine

exit

This command returns to the previous configuration mode or exit the configuration program.

Default Setting

None

Command Mode

Any

Example

This example shows how to return to the Privileged Exec mode from the Global Configuration mode, and then quit the CLI session:

```
Console(config)#exit
Console#exit

Press ENTER to start session
User Access Verification

Username:
```

quit

This command exits the configuration program.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

The **quit** and **exit** commands can both exit the configuration program.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to quit a CLI session:

```
Console#quit

Press ENTER to start session

User Access Verification

Username:
```

System Management Commands

These commands are used to control system logs, passwords, user names, browser configuration options, and display or configure a variety of other system information.

Command Group	Function	Page
Device Designation	Configures information that uniquely identifies this switch	3-34
User Access	Configures the basic user names and passwords for management access	3-35
IP Filter	Configures IP addresses that are allowed management access	3-38
Web Server	Enables management access via a web browser	3-41
Secure Shell	Provides secure replacement for Telnet	3-45
Event Logging	Controls logging of error messages	3-58
SMTP Alerts	Configures SMTP email alerts	3-65
Time (System Clock)	Sets the system clock automatically via NTP/SNTP server or manually	3-70
System Status	Displays system configuration, active managers, and version information	3-78
Frame Size	Enables support for jumbo frames	3-84

Downloaded from www.Manualslib.com manuals search engine

Device Designation Commands

Command	Function	Mode	Page
prompt	Customizes the prompt used in PE and NE mode	GC	3-34
hostname	Specifies the host name for the switch	GC	3-34
snmp-server contact	Sets the system contact string	GC	3-148
snmp-server location	Sets the system location string	GC	3-149

prompt

This command customizes the CLI prompt. Use the **no** form to restore the default prompt.

Syntax

prompt *string*
no prompt

string - Any alphanumeric string to use for the CLI prompt. (Maximum length: 255 characters)

Default Setting

Console

Command Mode

Global Configuration

Example

```
Console(config)#prompt RD2
RD2(config)#
```

hostname

This command specifies or modifies the host name for this device. Use the **no** form to restore the default host name.

Downloaded from www.Manualslib.com manuals search engine

Syntax

hostname *name*
no hostname

name - The name of this host. (Maximum length: 255 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#hostname RD#1
Console(config)#
```

User Access Commands

The basic commands required for management access are listed in this section. This switch also includes other options for password checking via the console or a Telnet connection (page 3-15), user authentication via a remote authentication server (page 3-92), and host access authentication for specific ports (page 3-104).

Command	Function	Mode	Page
username	Establishes a user name-based authentication system at login	GC	3-35
enable password	Sets a password to control access to the Privileged Exec level	GC	3-37

username

This command adds named users, requires authentication at login, specifies or changes a user's password (or specify that no password is required), or specifies or changes a user's access level. Use the **no** form to remove a user name.

Downloaded from www.Manualslib.com manuals search engine

Syntax

username *name* {**access-level** *level* | **nopassword** | **password** {**0** | **7**} *password*}
no username *name*

- *name* - The name of the user.
  (Maximum length: 8 characters, case sensitive. Maximum users: 16)
- **access-level** *level* - Specifies the user level.
  The device has two predefined privilege levels:
  0: Normal Exec, **15**: Privileged Exec.
- **nopassword** - No password is required for this user to log in.
- {**0** | **7**} - 0 means plain password, 7 means encrypted password.
- **password** *password* - The authentication password for the user.
  (Maximum length: 8 characters plain text, 32 encrypted, case sensitive)

Default Setting

- The default access level is Normal Exec.
- The factory defaults for the user names and passwords are:

username	access-level	password
guest	0	guest
admin	15	admin

Command Mode

Global Configuration

Command Usage

The encrypted password is required for compatibility with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from a TFTP server. There is no need for you to manually configure encrypted passwords.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how the set the access level and password for a user.

```
Console(config)#username bob access-level 15
Console(config)#username bob password 0 smith
Console(config)#
```

enable password

After initially logging onto the system, you should set the Privileged Exec password. Remember to record it in a safe place. This command controls access to the Privileged Exec level from the Normal Exec level. Use the **no** form to reset the default password.

Syntax

enable password [**level** *level*] {**0** | **7**} *password*
no enable password [**level** *level*]

- **level** *level* - Level 15 for Privileged Exec. (Levels 0-14 are not used.)
- {**0** | **7**} - 0 means plain password, 7 means encrypted password.
- *password* - password for this privilege level.

(Maximum length: 8 characters plain text, 32 encrypted, case sensitive)

Default Setting

- The default is level 15.
- The default password is "super"

Command Mode

Global Configuration

Command Usage

- You cannot set a null password. You will have to enter a password to change the command mode from Normal Exec to Privileged Exec with the **enable** command (page 3-27).
- The encrypted password is required for compatibility with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup or when downloading the

Downloaded from www.Manualslib.com manuals search engine

configuration file from a TFTP server. There is no need for you to manually configure encrypted passwords.

Example

```
Console(config)#enable password level 15 0 admin
Console(config)#
```

Related Commands

enable (3-27)

IP Filter Commands

Command	Function	Mode	Page
management	Configures IP addresses that are allowed management access	GC	3-38
show management	Displays the switch to be monitored or configured from a browser	PE	3-39

management

This command specifies the client IP addresses that are allowed management access to the switch through various protocols. Use the **no** form to restore the default setting.

Syntax

[**no**] **management** {**all-client** | **http-client** | **snmp-client** | **telnet-client**} *start-address* [*end-address*]

- **all-client** - Adds IP address(es) to the SNMP, web and Telnet groups.
- **http-client** - Adds IP address(es) to the web group.
- **snmp-client** - Adds IP address(es) to the SNMP group.
- **telnet-client** - Adds IP address(es) to the Telnet group.
- *start-address* - A single IP address, or the starting address of a range.
- *end-address* - The end address of a range.

Downloaded from www.Manualslib.com manuals search engine

Default Setting

All addresses

Command Mode

Global Configuration

Command Usage

- If anyone tries to access a management interface on the switch from an invalid address, the switch will reject the connection, enter an event message in the system log, and send a trap message to the trap manager.
- IP address can be configured for SNMP, web and Telnet access respectively. Each of these groups can include up to five different sets of addresses, either individual addresses or address ranges.
- When entering addresses for the same group (i.e., SNMP, web or Telnet), the switch will not accept overlapping address ranges. When entering addresses for different groups, the switch will accept overlapping address ranges.
- You cannot delete an individual address from a specified range. You must delete the entire range, and reenter the addresses.
- You can delete an address range just by specifying the start address, or by specifying both the start address and end address.

Example

This example restricts management access to the indicated addresses.

```
Console(config)#management all-client 192.168.1.19
Console(config)#management all-client 192.168.1.25 192.168.1.30
Console#
```

show management

This command displays the client IP addresses that are allowed management access to the switch through various protocols.

Syntax

show management {**all-client** | **http-client** | **snmp-client** | **telnet-client**}

Downloaded from www.Manualslib.com manuals search engine

- **all-client** - Adds IP address(es) to the SNMP, web and Telnet groups.
- **http-client** - Adds IP address(es) to the web group.
- **snmp-client** - Adds IP address(es) to the SNMP group.
- **telnet-client** - Adds IP address(es) to the Telnet group.

Command Mode

Global Configuration

Example

```
Console#show management all-client
Management Ip Filter
 Http-Client:
   Start ip address      End ip address
-----------------------------------------------
1. 192.168.1.19          192.168.1.19
2. 192.168.1.25          192.168.1.30

 Snmp-Client:
   Start ip address      End ip address
-----------------------------------------------
1. 192.168.1.19          192.168.1.19
2. 192.168.1.25          192.168.1.30

 Telnet-Client:
   Start ip address      End ip address
-----------------------------------------------
1. 192.168.1.19          192.168.1.19
2. 192.168.1.25          192.168.1.30

Console#
```


Downloaded from www.Manualslib.com manuals search engine

Web Server Commands

Command	Function	Mode	Page
ip http port	Specifies the port to be used by the web browser interface	GC	3-41
ip http server	Allows the switch to be monitored or configured from a browser	GC	3-42
ip http secure-server	Enables HTTPS/SSL for encrypted communications	GC	3-42
ip http secure-port	Specifies the UDP port number for HTTPS/SSL	GC	3-44

ip http port

This command specifies the TCP port number used by the web browser interface. Use the **no** form to use the default port.

Syntax

ip http port *port-number*
no ip http port

port-number - The TCP port to be used by the browser interface. (Range: 1-65535)

Default Setting

80

Command Mode

Global Configuration

Example

```
Console(config)#ip http port 769
Console(config)#
```

Related Commands

ip http server (3-42)

Downloaded from www.Manualslib.com manuals search engine

ip http server

This command allows this device to be monitored or configured from a browser. Use the **no** form to disable this function.

Syntax

[**no**] **ip http server**

Default Setting

Enabled

Command Mode

Global Configuration

Example

```
Console(config)#ip http server
Console(config)#
```

Related Commands

ip http port (3-41)

ip http secure-server

This command enables the secure hypertext transfer protocol (HTTPS) over the Secure Socket Layer (SSL), providing secure access (i.e., an encrypted connection) to the switch's web interface. Use the **no** form to disable this function.

Syntax

[**no**] **ip http secure-server**

Default Setting

Enabled

Command Mode

Global Configuration

Downloaded from www.Manualslib.com manuals search engine

Command Usage

- Both HTTP and HTTPS service can be enabled independently on the switch. However, you cannot configure the HTTP and HTTPS servers to use the same UDP port.
- If you enable HTTPS, you must indicate this in the URL that you specify in your browser: **https**://*device*[:*port_number*]
- When you start HTTPS, the connection is established in this way:
  - The client authenticates the server using the server's digital certificate.
  - The client and server negotiate a set of security protocols to use for the connection.
  - The client and server generate session keys for encrypting and decrypting data.
- The client and server establish a secure encrypted connection.

  A padlock icon should appear in the status bar for Internet Explorer 5.x and Netscape Navigator 4.x or later versions.
- The following web browsers and operating systems currently support HTTPS:

Web Browser	Operating System
Internet Explorer 5.0 or later	Windows 98,Windows NT (with service pack 6a), Windows 2000, Windows XP
Netscape Navigator 4.76 or later	Windows 98,Windows NT (with service pack 6a), Windows 2000, Windows XP, Solaris 2.6

- To specify a secure-site certificate, see "Replacing the Default Secure-site Certificate" on page 3-49. Also refer to the **copy** command on page 3-85.

Example

```
Console(config)#ip http secure-server
Console(config)#
```

Related Commands

ip http secure-port (3-44)

Downloaded from www.Manualslib.com manuals search engine

copy tftp https-certificate (3-85)

ip http secure-port

This command specifies the UDP port number used for HTTPS/SSL connection to the switch's web interface. Use the **no** form to restore the default port.

Syntax

ip http secure-port *port_number*
no ip http secure-port

port_number – The UDP port used for HTTPS/SSL. (Range: 1-65535)

Default Setting

443

Command Mode

Global Configuration

Command Usage

- You cannot configure the HTTP and HTTPS servers to use the same port.
- If you change the HTTPS port number, clients attempting to connect to the HTTPS server must specify the port number in the URL, in this format:
  https://*device***:***port_number*

Example

```
Console(config)#ip http secure-port 1000
Console(config)#
```

Related Commands

ip http secure-server (3-42)

Downloaded from www.Manualslib.com manuals search engine

Secure Shell Commands

The Berkley-standard includes remote access tools originally designed for Unix systems. Some of these tools have also been implemented for Microsoft Windows and other environments. These tools, including commands such as *rlogin* (remote login), *rsh* (remote shell), and *rcp* (remote copy), are not secure from hostile attacks.

The Secure Shell (SSH) includes server/client applications intended as a secure replacement for the older Berkley remote access tools. SSH can also provide remote management access to this switch as a secure replacement for Telnet. When a client contacts the switch via the SSH protocol, the switch uses a public-key that the client must match along with a local user name and password for access authentication. SSH also encrypts all data transfers passing between the switch and SSH-enabled management station clients, and ensures that data traveling over the network arrives unaltered.

This section describes the commands used to configure the SSH server. However, note that you also need to install a SSH client on the management station when using this protocol to configure the switch.

Note: The switch supports both SSH Version 1.5 and 2.0.

Command	Function	Mode	Page
ip ssh server	Enables the SSH server on the switch	GC	3-48
ip ssh timeout	Specifies the authentication timeout for the SSH server	GC	3-49
ip ssh authentication-retries	Specifies the number of retries allowed by a client	GC	3-50
ip ssh server-key size	Sets the SSH server key size	GC	3-51
copy tftp public-key	Copies the user's public key from a TFTP server to the switch	PE	3-85
delete public-key	Deletes the public key for the specified user	PE	3-51

Downloaded from www.Manualslib.com manuals search engine

Command	Function	Mode	Page
ip ssh crypto host-key generate	Generates the host key	PE	3-52
ip ssh crypto zeroize	Clear the host key from RAM	PE	3-53
ip ssh save host-key	Saves the host key from RAM to flash memory	PE	3-54
disconnect	Terminates a line connection	PE	3-25
show ip ssh	Displays the status of the SSH server and the configured values for authentication timeout and retries	PE	3-54
show ssh	Displays the status of current SSH sessions	PE	3-55
show public-key	Shows the public key for the specified user or for the host	PE	3-56
show users	Shows SSH users, including privilege level and public key type	PE	3-83

The SSH server on this switch supports both password and public key authentication. If password authentication is specified by the SSH client, then the password can be authenticated either locally or via a RADIUS or TACACS+ remote authentication server, as specified by the **authentication login** command on page 3-93. If public key authentication is specified by the client, then you must configure authentication keys on both the client and the switch as described in the following section. Note that regardless of whether you use public key or password authentication, you still have to generate authentication keys on the switch and enable the SSH server.

To use the SSH server, complete these steps:

1. Generate a Host Key Pair – Use the **ip ssh crypto host-key generate** command to create a host public/private key pair.

2. Provide Host Public Key to Clients – Many SSH client programs automatically import the host public key during the initial connection setup with the switch. Otherwise, you need to manually create a

Downloaded from www.Manualslib.com manuals search engine

known hosts file on the management station and place the host public key in it. An entry for a public key in the known hosts file would appear similar to the following example:

```
10.1.0.54 1024 35 15684995401867669259333946775054617325313674890836547254
150202455931998685443583616519999233297817660658309561082591321289023376546801726272571413428762941301196195566782 595664104869574278881462065194174677298486546861571773939016477935594230357741309802273708779454524083971752646358058176716709574804776117
```

3. Import Client's Public Key to the Switch – Use the **copy tftp public-key** command to copy a file containing the public key for all the SSH client's granted management access to the switch. The clients are subsequently authenticated using these keys. The current firmware only accepts public key files based on standard UNIX format as shown in the following example:

```
1024 35 134108168560989392104094492015542534763164192187295892114317388005555361616310517759408386863110929123222682851925437460310093718772119969631781366277414168985132049117204830339254324101637997592371449011938006090253948408482717819437228840253311595213486102290297898272135326713162943253281891504530639391664 3 steve@192.168.1.19
```

4. Set the Optional Parameters – Set other optional parameters, including the authentication timeout, the number of retries, and the server key size.

5. Enable SSH Service – Use the **ip ssh server** command to enable the SSH server on the switch.

6. Configure Challenge-Response Authentication – When an SSH client attempts to contact the switch, the SSH server uses the host key pair to negotiate a session key and encryption method. Only clients that have a private key corresponding to the public keys stored on the switch can gain access. The following exchanges take place during this process:

a. The client sends its public key to the switch.
b. The switch compares the client's public key to those stored in memory.

Downloaded from www.Manualslib.com manuals search engine

c. If a match is found, the switch uses the public key to encrypt a random sequence of bytes, and sends this string to the client.
d. The client uses its private key to decrypt the bytes, and sends the decrypted bytes back to the switch.
e. The switch compares the decrypted bytes to the original bytes it sent. If the two sets match, this means that the client's private key corresponds to an authorized public key, and the client is authenticated.

Note: To use SSH with only password authentication, the host public key must still be given to the client, either during initial connection or manually entered into the known host file. However, you do not need to configure the client's keys.

ip ssh server

Use this command to enable the Secure Shell (SSH) server on this switch. Use the **no** form to disable this service.

Syntax

ip ssh server
no ip ssh server

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- The SSH server supports up to four client sessions. The maximum number of client sessions includes both current Telnet sessions and SSH sessions.
- The SSH server uses DSA or RSA for key exchange when the client first establishes a connection with the switch, and then negotiates with the client to select either DES (56-bit) or 3DES (168-bit) for data encryption.
- You must generate the host key before enabling the SSH server.

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console#ip ssh crypto host-key generate dsa
Console#configure
Console(config)#ip ssh server
Console(config)#
```

Related Commands

ip ssh crypto host-key generate (3-52)
show ssh (3-55)

ip ssh timeout

Use this command to configure the timeout for the SSH server. Use the **no** form to restore the default setting.

Syntax

ip ssh timeout *seconds*
no ip ssh timeout

seconds – The timeout for client response during SSH negotiation. (Range: 1-120)

Default Setting

10 seconds

Command Mode

Global Configuration

Command Usage

The **timeout** specifies the interval the switch will wait for a response from the client during the SSH negotiation phase. Once an SSH session has been established, the timeout for user input is controlled by the **exec-timeout** command for vty sessions.

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console(config)#ip ssh timeout 60
Console(config)#
```

Related Commands

exec-timeout (3-19)
show ip ssh (3-54)

ip ssh authentication-retries

Use this command to configure the number of times the SSH server attempts to reauthenticate a user. Use the **no** form to restore the default setting.

Syntax

ip ssh authentication-retries *count*
no ip ssh authentication-retries

count – The number of authentication attempts permitted after which the interface is reset. (Range: 1-5)

Default Setting

3

Command Mode

Global Configuration

Example

```
Console(config)#ip ssh authentication-retires 2
Console(config)#
```

Related Commands

show ip ssh (3-54)

Downloaded from www.Manualslib.com manuals search engine

ip ssh server-key size

Use this command to set the SSH server key size. Use the **no** form to restore the default setting.

Syntax

ip ssh server-key size *key-size*
no ip ssh server-key size

key-size – The size of server key. (Range: 512-896 bits)

Default Setting

768 bits

Command Mode

Global Configuration

Command Usage

- The server key is a private key that is never shared outside the switch.
- The host key is shared with the SSH client, and is fixed at 1024 bits.

Example

```
Console(config)#ip ssh server-key size 512
Console(config)#
```

delete public-key

Use this command to delete the specified user's public key.

Syntax

delete public-key *username* [**dsa** | **rsa**]

- *username* – Name of an SSH user. (Range: 1-8 characters)
- **dsa** – DSA public key type.
- **rsa** – RSA public key type.

Default Setting

Deletes both the DSA and RSA key.

Downloaded from www.Manualslib.com manuals search engine

Command Mode

Privileged Exec

Example

```
Console#delete public-key admin dsa
Console#
```

ip ssh crypto host-key generate

Use this command to generate the host key pair (i.e., public and private).

Syntax

ip ssh crypto host-key generate [**dsa** | **rsa**]

- **dsa** – DSA key type.
- **rsa** – RSA key type.

Default Setting

Generates both the DSA and RSA key pairs.

Command Mode

Privileged Exec

Command Usage

- This command stores the host key pair in memory (i.e., RAM). Use the **ip ssh save host-key** command to save the host key pair to flash memory.
- Some SSH client programs automatically add the public key to the known hosts file as part of the configuration process. Otherwise, you must manually create a known hosts file and place the host public key in it.
- The SSH server uses this host key to negotiate a session key and encryption method with the client trying to connect to it.

Example

```
Console#ip ssh crypto host-key generate dsa
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Related Commands

ip ssh crypto zeroize (3-53)
ip ssh save host-key (3-54)

ip ssh crypto zeroize

Use this command to clear the host key from memory (i.e. RAM).

Syntax

ip ssh crypto zeroize [**dsa** | **rsa**]

- **dsa** – DSA key type.
- **rsa** – RSA key type.

Default Setting

Clears both the DSA and RSA key.

Command Mode

Privileged Exec

Command Usage

- This command clears the host key from volatile memory (RAM). Use the **no ip ssh save host-key** command to clear the host key from flash memory.
- The SSH server must be disabled before you can execute this command.

Example

```
Console#ip ssh crypto zeroize dsa
Console#
```

Related Commands

ip ssh crypto host-key generate (3-52)
ip ssh save host-key (3-54)
no ip ssh server (3-48)

Downloaded from www.Manualslib.com manuals search engine

ip ssh save host-key

Use this command to save host key from RAM to flash memory.

Syntax

ip ssh save host-key [**dsa** | **rsa**]

- **dsa** – DSA key type.
- **rsa** – RSA key type.

Default Setting

Saves both the DSA and RSA key.

Command Mode

Privileged Exec

Example

```
Console#ip ssh save host-key dsa
Console#
```

Related Commands

ip ssh crypto host-key generate (3-52)

show ip ssh

Use this command to display the connection settings used when authenticating client access to the SSH server.

Command Mode

Privileged Exec

Example

```
Console#show ip ssh
SSH Enabled - version 1.99
Negotiation timeout: 120 secs; Authentication retries: 3
Server key size: 768 bits
Console#
```


Downloaded from www.Manualslib.com manuals search engine

show ssh

Use this command to display the current SSH server connections.

Command Mode

Privileged Exec

Example

```
Console#show ssh
Connection Version State                Username Encryption
  0          2.0   Session-Started      admin    ctos aes128-cbc-hmac-md5
                                                 stoc aes128-cbc-hmac-md5

Console#
```

Field	Description
Session	The session number. (Range: 0-3)
Version	The Secure Shell version number.
State	The authentication negotiation state. (Values: Negotiation-Started, Authentication-Started, Session-Started)
Username	The user name of the client.

Downloaded from www.Manualslib.com manuals search engine

Field	Description
Encryption	The encryption method is automatically negotiated between the client and server. Options for SSHv1.5 include: DES, 3DES Options for SSHv2.0 can include different algorithms for the client-to-server (ctos) and server-to-client (stoc): aes128-cbc-hmac-sha1 aes192-cbc-hmac-sha1 aes256-cbc-hmac-sha1 3des-cbc-hmac-sha1 blowfish-cbc-hmac-sha1 aes128-cbc-hmac-md5 aes192-cbc-hmac-md5 aes256-cbc-hmac-md5 3des-cbc-hmac-md5 blowfish-cbc-hmac-md5 *Terminology:* DES – Data Encryption Standard (56-bit key) 3DES – Triple-DES (Uses three iterations of DES, 112-bit key) aes – Advanced Encryption Standard (160 or 224-bit key) blowfish – Blowfish (32-448 bit key) cbc – cypher-block chaining sha1 – Secure Hash Algorithm 1 (160-bit hashes) md5 – Message Digest algorithm number 5 (128-bit hashes)

show public-key

Use this command to show the public key for the specified user or for the host.

Syntax

show public-key [**user** [*username*] | **host**]

username – Name of an SSH user. (Range: 1-8 characters)

Default Setting

Shows all public keys.

Downloaded from www.Manualslib.com manuals search engine

Command Mode

Privileged Exec

Command Usage

- If no parameters are entered, all keys are displayed. If the user keyword is entered, but no user name is specified, then the public keys for all users are displayed.
- When an RSA key is displayed, the first field indicates the size of the host key (e.g., 1024), the second field is the encoded public exponent (e.g., 35), and the last string is the encoded modulus. When a DSA key is displayed, the first field indicates that the encryption method used by SSH is based on the Digital Signature Standard (DSS), and the last string is the encoded modulus.

Example

```
Console#show public-key host
Host:
RSA:
1024 35
156849954018676692593339467750546173253136748908365472541502024559319986854435836165199992332978176606583095861082591321289023376546801726272571413428762941301196195566782595664104869574278881462065194174677298486546861571773939016477935594230357741309802273708779454524083971752646358058176716709574804776117
DSA:
ssh-dss AAAB3NzaC1kc3MAAACBAPWKZTPbsRIB8ydEXcxM3dyV/yrDbKStIlnzD/Dg0h2HxcYV44sXZ2JXhamLK6P8bvuiyacWbUW/a4PAtp1KMSdqsKeh3hKoA3vRRSy1N2XFfAKxl5fwFfvJlPdOkFgzLGMinvSNYQwiQXbKTBH0Z4mUZpE85PWxDZMaCNBPjBrRAAAAFQChb4vsdfQGNIjwbvwrNLaQ77isiwAAAIEAsy5YWDC99ebYHNRj5kh47wY4i8cZvH+/p9cnrfwFTMU01VFDly3IR2G395NLy5Qd7ZDxfA9mCOfT/yyEfbobMJZi8oGCstSNOxrZZVnMqWrTYfdrKX7YKBw/Kjw6BmiFq7O+jAhf1Dg45loAc27s6TLdtny1wRq/ow2eTCD5nekAAACBAJ8rMccXTxHLFAczWS7EjOyDbsloBfPuSAb4oAsyjKXKVYNLQkTLZfcFRu41bS2KV5LAwecsigF/+DjKGWtPNIQqabKgYCw2o/dVzX4Gg+yqdTlYmGA7fHGm8ARGeiG4ssFKy4Z6DmYPXFum1Yg0fhLwuHpOSKdxT3kk475S7w0W
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Event Logging Commands

Command	Function	Mode	Page
logging on	Controls logging of error messages	GC	3-58
logging history	Limits syslog messages saved to switch memory based on severity	GC	3-59
logging host	Adds a syslog server host IP address that will receive logging messages	GC	3-60
logging facility	Sets the facility type for remote logging of syslog messages	GC	3-61
logging trap	Limits syslog messages saved to a remote server based on severity	GC	3-62
clear logging	Clears messages from the logging buffer	PE	3-62
show logging	Displays the state of logging	PE	3-63

logging on

This command controls logging of error messages, sending debug or error messages to switch memory. The **no** form disables the logging process.

Syntax

[**no**] **logging on**

Default Setting

None

Command Mode

Global Configuration

Command Usage

The logging process controls error messages saved to switch memory. You can use the **logging history** command to control the type of error messages that are stored.

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console(config)#logging on
Console(config)#
```

Related Commands

logging history (3-59)
clear logging (3-62)

logging history

This command limits syslog messages saved to switch memory based on severity. The **no** form returns the logging of syslog messages to the default level.

Syntax

logging history {**flash** | **ram**} *level*
no logging history {**flash** | **ram**}

- **flash** - Event history stored in flash memory (i.e., permanent memory).
- **ram** - Event history stored in temporary RAM (i.e., memory flushed on power reset).

Downloaded from www.Manualslib.com manuals search engine

- *level* - One of the level arguments listed below. Messages sent include the selected level down to level 0. (Range: 0-7)

Level Argument	Level	Description
debugging	7	Debugging messages
informational	6	Informational messages only
notifications	5	Normal but significant condition, such as cold start
warnings	4	Warning conditions (e.g., return false, unexpected return)
errors	3	Error conditions (e.g., invalid input, default used)

* There are only Level 2, 5 and 6 error messages for the current firmware release.

critical	2	Critical conditions (e.g., memory allocation, or free memory error - resource exhausted)
alerts	1	Immediate action needed
emergencies	0	System unusable

Default Setting

Flash: errors (level 3 - 0)
RAM: warnings (level 7 - 0)

Command Mode

Global Configuration

Command Usage

The message level specified for flash memory must be a higher priority (i.e., numerically lower) than that specified for RAM.

Example

```
Console(config)#logging history ram 0
Console(config)#
```

logging host

This command adds a syslog server host IP address that will receive

Downloaded from www.Manualslib.com manuals search engine

Syntax

[no] logging host *host_ip_address*

host_ip_address - The IP address of a syslog server.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- By using this command more than once you can build up a list of host IP addresses.
- The maximum number of host IP addresses allowed is five.

Example

```
Console(config)#logging host 10.1.0.3
Console(config)#
```

logging facility

This command sets the facility type for remote logging of syslog messages. Use the **no** form to return the type to the default.

Syntax

[no] logging facility *type*

type - A number that indicates the facility used by the syslog server to dispatch log messages to an appropriate service. (Range: 16-23)

Default Setting

23

Command Mode

Global Configuration

Downloaded from www.Manualslib.com manuals search engine

Command Usage

The command specifies the facility type tag sent in syslog messages. (See RFC 3164.) This type has no effect on the kind of messages reported by the switch. However, it may be used by the syslog server to sort messages or to store messages in the corresponding database.

Example

```
Console(config)#logging facility 19
Console(config)#
```

logging trap

This command limits syslog messages saved to a remote server based on severity. Use the **no** form to return the remote logging of syslog messages to the default level.

Syntax

[**no**] **logging trap** *level*

level - One of the level arguments listed below. Messages sent include the selected level up through level 0. (Refer to the table on page 3-59.)

Default Setting

Level 3 - 0

Command Mode

Global Configuration

Example

```
Console(config)#logging trap 4
Console(config)#
```

clear logging

This command clears messages from the log buffer.

Downloaded from www.Manualslib.com manuals search engine

Syntax

clear logging [**flash** | **ram**]

- **flash** - Event history stored in flash memory (i.e., permanent memory).
- **ram** - Event history stored in temporary RAM (i.e., memory flushed on power reset).

Default Setting

Flash and RAM

Command Mode

Privileged Exec

Example

```
Console#clear logging
Console#
```

Related Commands

show logging (3-63)

show logging

This command displays the logging configuration, along with any system and event messages stored in memory.

Syntax

show logging {**flash** | **ram** | **sendmail** | **trap**}

- **flash** - Event history stored in flash memory (i.e., permanent memory).
- **ram** - Event history stored in temporary RAM (i.e., memory flushed on power reset).
- **sendmail** - Displays settings for the SMTP event handler (page 3-70).
- **trap** - Displays settings for the trap function.

Downloaded from www.Manualslib.com manuals search engine

Default Setting

None

Command Mode

Privileged Exec

Example

The following example shows that system logging is enabled, the message level for flash memory is "errors" (i.e., default level 3 - 0), the message level for RAM is "debugging" (i.e., default level 7 - 0), and lists one sample error.

```
Console#show logging flash
Syslog logging: Enable
History logging in FLASH: level errors
[0] 0:0:5 1/1/1 "PRI_MGR_InitDefault function fails."
   level: 3, module: 13, function: 0, and event no.: 0
Console#show logging ram
Syslog logging: Enable
History logging in RAM: level debugging
[0] 0:0:5 1/1/1 PRI_MGR_InitDefault function fails."
   level: 3, module: 13, function: 0, and event no.: 0
Console#
```

Field	Description
Syslog logging	Shows if system logging has been enabled via the **logging on** command.
History logging in FLASH	The message level(s) reported based on the **logging history** command.
History logging in RAM	The message level(s) reported based on the **logging history** command.
Messages	Any system and event messages stored in memory.

Downloaded from www.Manualslib.com manuals search engine

The following example displays settings for the trap function.

```
Console#show logging trap
Syslog logging: Enable
REMOTELOG status: disable
REMOTELOG facility type: local use 7
REMOTELOG level type: Debugging messages
REMOTELOG server IP address: 1.2.3.4
REMOTELOG server IP address: 0.0.0.0
REMOTELOG server IP address: 0.0.0.0
REMOTELOG server IP address: 0.0.0.0
REMOTELOG server IP address: 0.0.0.0
Console#
```

Field	Description
Syslog logging	Shows if system logging has been enabled via the **logging on** command.
REMOTELOG status	Shows if remote logging has been enabled via the **logging trap** command.
REMOTELOG facility type	The facility type for remote logging of syslog messages as specified in the **logging facility** command.
REMOTELOG level type	The severity threshold for syslog messages sent to a remote server as specified in the **logging trap** command.
REMOTELOG server IP address	The address of syslog servers as specified in the **logging host** command.

Related Commands

show logging sendmail (3-70)

SMTP Alert Commands

Configures SMTP event handling, and forwarding of alert messages to the specified SMTP servers and email recipients.

Command	Function	Mode	Page
logging sendmail host	SMTP servers to receive alert messages	GC	3-66
logging sendmail level	Severity threshold used to trigger alert messages	GC	3-67

Downloaded from www.Manualslib.com manuals search engine

Command	Function	Mode	Page
logging sendmail source-email	Email address used for "From" field of alert messages	GC	3-68
logging sendmail destination-email	Email recipients of alert messages	GC	3-68
logging sendmail	Enables SMTP event handling	GC	3-69
show logging sendmail	Displays SMTP event handler settings	NE, PE	3-70

logging sendmail host

This command specifies SMTP servers that will be sent alert messages. Use the **no** form to remove an SMTP server.

Syntax

[**no**] **logging sendmail host** *ip_address*

ip_address - IP address of an SMTP server that will be sent alert messages for event handling.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- You can specify up to three SMTP servers for event handing. However, you must enter a separate command to specify each server.
- To send email alerts, the switch first opens a connection, sends all the email alerts waiting in the queue one by one, and finally closes the connection.
- To open a connection, the switch first selects the server that successfully sent mail during the last connection, or the first server configured by this command. If it fails to send mail, the switch selects the next server in the list and tries to send mail again. If it still fails, the system will repeat the process at a periodic interval. (A trap will be

Downloaded from www.Manualslib.com manuals search engine

triggered if the switch cannot successfully open a connection.)

Example

```
Console(config)#logging sendmail host 192.168.1.19
Console(config)#
```

logging sendmail level

This command sets the severity threshold used to trigger alert messages.

Syntax

logging sendmail level *level*

level - One of the system message levels (page 3-59). Messages sent include the selected level down to level 0. (Range: 0-7; Default: 7)

Default Setting

Level 7

Command Mode

Global Configuration

Command Usage

The specified level indicates an event threshold. All events at this level or higher will be sent to the configured email recipients. (For example, using Level 7 will report all events from level 7 to level 0.)

Example

This example will send email alerts for system errors from level 3 through 0.

```
Console(config)#logging sendmail level 3
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

logging sendmail source-email

This command sets the email address used for the "From" field in alert messages.

Syntax

logging sendmail source-email *email-address*

email-address - The source email address used in alert messages. (Range: 1-41 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

You may use an symbolic email address that identifies the switch, or the address of an administrator responsible for the switch.

Example

This example will send email alerts for system errors from level 3 through 0.

```
Console(config)#logging sendmail source-email bill@this-company.com
Console(config)#
```

logging sendmail destination-email

This command specifies the email recipients of alert messages. Use the **no** form to remove a recipient.

Syntax

[**no**] **logging sendmail destination-email** *email-address*

email-address - The source email address used in alert messages. (Range: 1-41 characters)

Downloaded from www.Manualslib.com manuals search engine

Default Setting

None

Command Mode

Global Configuration

Command Usage

You can specify up to five recipients for alert messages. However, you must enter a separate command to specify each recipient.

Example

```
Console(config)#logging sendmail destination-email ted@this-company.com
Console(config)#
```

logging sendmail

This command enables SMTP event handling. Use the **no** form to disable this function.

Syntax

[**no**] **logging sendmail**

Default Setting

Disabled

Command Mode

Global Configuration

Example

```
Console(config)#logging sendmail
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

show logging sendmail

This command displays the settings for the SMTP event handler.

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show logging sendmail
SMTP servers
-------------------------------------------------
192.168.1.19
SMTP minimum severity level: 7

SMTP destination email addresses
-------------------------------------------------
ted@this-company.com

SMTP source email address: bill@this-company.com

SMTP status: Enable

Console#
```

Time Commands

The system clock can be dynamically set by polling a set of specified time servers (NTP or SNTP), or by using information broadcast by local time servers.

Command	Function	Mode	Page
sntp client	Accepts time from specified time servers	GC	3-71
sntp server	Specifies one or more time servers	GC	3-72
sntp poll	Sets the interval at which the client polls for time	GC	3-73
sntp broadcast client	Accepts time from any time broadcast server	GC	3-74
show sntp	Shows current SNTP configuration settings	NE, PE	3-75
clock timezone	Sets the time zone for the switch's internal clock	GC	3-75

Downloaded from www.Manualslib.com manuals search engine

Command	Function	Mode	Page
calendar set	Sets the system date and time	PE	3-76
show calendar	Displays the current date and time setting	NE, PE	3-77

sntp client

This command enables SNTP client requests for time synchronization from NTP or SNTP time servers specified with the **sntp servers** command. Use the **no** form to disable SNTP client requests.

Syntax

[**no**] **sntp client**

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- The time acquired from time servers is used to record accurate dates and times for log events. Without SNTP, the switch only records the time starting from the factory default set at the last bootup (i.e., 00:00:00, Jan. 1, 2001).
- This command enables client time requests to time servers specified via the **sntp servers** command. It issues time synchronization requests based on the interval set via the **sntp poll** command.
- The SNTP time query method is set to client mode when the first **sntp client** command is issued. However, if the **sntp broadcast client** command is issued, then the **no sntp broadcast client** command must be used to return the switch to SNTP client mode.

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console(config)#sntp server 10.1.0.19
Console(config)#sntp poll 60
Console(config)#sntp client
Console(config)#end
Console#show sntp
Current time:  Dec 23 02:52:44 2002
Poll interval: 60
Current mode: unicast
Console#
```

Related Commands

sntp server (3-72)
sntp poll (3-73)
sntp broadcast client (3-74)
show sntp (3-75)

sntp server

This command sets the IP address of the servers to which SNTP time requests are issued. Use the this command with no arguments to clear all time servers from the current list.

Syntax

sntp server [*ip1* [*ip2* [*ip3*]]]

ip - IP address of an time server (NTP or SNTP).
(Range: 1 - 3 addresses)

Default Setting

None

Command Mode

Global Configuration

Downloaded from www.Manualslib.com manuals search engine

Command Usage

This command specifies time servers from which the switch will poll for time updates when set to SNTP client mode. The client will poll the time servers in the order specified until a response is received. It issues time synchronization requests based on the interval set via the **sntp poll** command.

Example

```
Console(config)#sntp server 10.1.0.19
Console#
```

Related Commands

sntp client (3-71)
sntp poll (3-73)
show sntp (3-75)

sntp poll

This command sets the interval between sending time requests when the switch is set to SNTP client mode. Use the **no** form to restore to the default.

Syntax

sntp poll *seconds*
no sntp poll

seconds - Interval between time requests. (Range: 16-16384 seconds)

Default Setting

16 seconds

Command Mode

Global Configuration

Command Usage

This command is only applicable when the switch is set to SNTP client mode.

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console(config)#sntp poll 60
Console#
```

Related Commands

sntp client (3-71)

sntp broadcast client

This command synchronizes the switch's clock based on time broadcast from time servers (using the multicast address 224.0.1.1). Use the **no** form to disable SNTP broadcast client mode.

Syntax

[no] sntp broadcast client

Default Setting

Disabled

Command Mode

Global Configuration

Example

```
Console(config)#sntp broadcast client
Console#
```


Downloaded from www.Manualslib.com manuals search engine

show sntp

This command displays the current time and configuration settings for the SNTP client, and indicates whether or not the local time has been properly updated.

Command Mode

Normal Exec, Privileged Exec

Command Usage

This command displays the current time, the poll interval used for sending time synchronization requests (when the switch is set to SNTP client mode), and the current SNTP mode (i.e., client or broadcast).

Example

```
Console#show sntp
Current time:  Dec 23 05:13:28 2002
Poll interval: 16
Current mode:  unicast
```

clock timezone

This command sets the time zone for the switch's internal clock.

Syntax

clock timezone *name* **hour** *hours* **minute** *minutes* {**before-utc** | **after-utc**}

- *name* - Name of timezone, usually an acronym. (Range: 1-29 characters)
- *hours* - Number of hours before/after UTC. (Range: 1-12 hours)
- *minutes* - Number of minutes before/after UTC. (Range: 0-59 minutes)
- **before-utc** - Sets the local time zone before (east) of UTC.
- **after-utc** - Sets the local time zone after (west) of UTC.

Default Setting

None

Downloaded from www.Manualslib.com manuals search engine

Command Mode

Global Configuration

Command Usage

This command sets the local time zone relative to the Coordinated Universal Time (UTC, formerly Greenwich Mean Time or GMT), based on the earth's prime meridian, zero degrees longitude. To display a time corresponding to your local time, you must indicate the number of hours and minutes your time zone is east (before) or west (after) of UTC.

Example

```
Console(config)#clock timezone Japan hours 8 minute 0 after-UTC
Console(config)#
```

Related Commands

show sntp (3-75)

calendar set

This command sets the system clock.

Syntax

calendar set *hour min sec* {*day month year* | *month day year*}

- *hour* - Hour in 24-hour format. (Range: 0 - 23)
- *min* - Minute. (Range: 0 - 59)
- *sec* - Second. (Range: 0 - 59)
- *day* - Day of month. (Range: 1 - 31)
- *month* - **january** | **february** | **march** | **april** | **may** | **june** | **july** | **august** | **september** | **october** | **november** | **december**
- *year* - Year (4-digit). (Range: 2001 - 2101)

Default Setting

None

Downloaded from www.Manualslib.com manuals search engine

Command Mode

Privileged Exec

Example

This example shows how to set the system clock to 15:12:34, February 1st, 2002.

```
Console#calendar set 15:12:34 1 February 2002
Console#
```

show calendar

This command displays the system clock.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show calendar set
 15:12:34 February 1 2002
Console#
```


Downloaded from www.Manualslib.com manuals search engine

System Status Commands

Command	Function	Mode	Page
show startup-config	Displays the contents of the configuration file (stored in flash memory) that is used to start up the system	PE	3-78
show running-config	Displays the configuration data currently in use	PE	3-79
show system	Displays system information	NE, PE	3-82
show users	Shows all active console and Telnet sessions, including user name, idle time, and IP address of Telnet clients	NE, PE	3-83
show version	Displays version information for the system	NE, PE	3-83

show startup-config

This command displays the configuration file stored in non-volatile memory that is used to start up the system.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- Use this command in conjunction with the **show running-config** command to compare the information in running memory to the information stored in non-volatile memory.
- This command displays settings for key command modes. Each mode group is separated by "!" symbols, and includes the configuration mode command, and corresponding commands. This command displays the following information:
  - SNMP community strings
  - Users (names and access levels)

Downloaded from www.Manualslib.com manuals search engine

- VLAN database (VLAN ID, name and state)
- VLAN configuration settings for each interface
- Multiple spanning tree instances (name and interfaces)
- IP address configured for VLANs
- Routing protocol configuration settings
- Spanning tree settings
- Any configured settings for the console port and Telnet

Example

```
Console#show startup-config
building startup-config, please wait.....
!
!
username admin access-level 15
username admin password 7 21232f297a57a5a743894a0e4a801fc3
!
username guest access-level 0
username guest password 7 084e0343a0486ff05530df6c705c8bb4
!
enable password level 15 7 1b3231655cebb7a1f783eddf27d254ca
!
snmp-server community public ro
snmp-server community private rw!
!
vlan database
 vlan 1 name DefaultVlan media ethernet state active
!
interface vlan 1
 ip address dhcp
!
line console
!
line vty
!
end

Console#
```

Related Commands

show running-config (3-79)

show running-config

This command displays the configuration information currently in use.

Downloaded from www.Manualslib.com manuals search engine

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- Use this command in conjunction with the **show startup-config** command to compare the information in running memory to the information stored in non-volatile memory.
- This command displays settings for key command modes. Each mode group is separated by "!" symbols, and includes the configuration mode command, and corresponding commands. This command displays the following information:
  - SNMP community strings
  - Users (names, access levels, and encrypted passwords)
  - VLAN database (VLAN ID, name and state)
  - VLAN configuration settings for each interface
  - Multiple spanning tree instances (name and interfaces)
  - IP address configured for VLANs
  - Routing protocol configuration settings
  - Spanning tree settings
  - Any configured settings for the console port and Telnet

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console#show running-config
building running-config, please wait.....
!
!
snmp-server community private rw
snmp-server community public ro
!
!
username admin access-level 15
username admin password 7 21232f297a57a5a743894a0e4a801fc3
username guest access-level 0
username guest password 7 084e0343a0486ff05530df6c705c8bb4
enable password level 15 7 1b3231655cebb7a1f783eddf27d254ca
!
vlan database
 vlan 1 name DefaultVlan media ethernet state active
!
spanning-tree mst-configuration
!
interface ethernet 1/1
 switchport allowed vlan add 1 untagged
 switchport native vlan 1
 lacp partner admin-key 0
 spanning-tree edge-port
.
.
.
!
interface vlan 1
 ip address 10.1.0.1 255.255.255.0
!
!
!
!
line console
!
line vty
!
end
Console#
```

Related Commands

show startup-config (3-78)

Downloaded from www.Manualslib.com manuals search engine

show system

This command displays system information.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

- For a description of the items shown by this command, refer to "Displaying System Information" on page 3-14.
- The POST results should all display "PASS." If any POST test indicates "FAIL," contact your distributor for assistance.

Example

```
Console#show system
System description: SMC Networks SMC8612XL3
System OID string: 1.3.6.1.4.1.202.20.33
System information
 System Up time: 0 days, 0 hours, 12 minutes, and 49.7 seconds
 System Name            : [NONE]
 System Location        : [NONE]
 System Contact         : [NONE]
 MAC address            : 00-30-F1-8F-D5-50
 Web server             : enable
 Web server port        : 80
 Web secure server      : enable
 Web secure server port : 443
 POST result
DUMMY Test 1.................PASS
UART LOOP BACK Test..........PASS
DRAM Test....................PASS
Timer Test...................PASS
PCI Device 1 Test............PASS
I2C bus Initialization.......PASS
RTC Initialization...........PASS
Switch Int Loopback test.....PASS

Done All Pass.
Console#
```


Downloaded from www.Manualslib.com manuals search engine

show users

Shows all active console and Telnet sessions, including user name, idle time, and IP address of Telnet client.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

The session used to execute this command is indicated by a "*" symbol next to the Line (i.e., session) index number.

Example

```
Console#show users
 Username accounts:
  Username Privilege Public-Key
  -------- --------- ----------
     admin        15       None
     guest         0       None

 Online users:
  Line        Username Idle time (h:m:s) Remote IP addr.
  ----------- -------- ----------------- ---------------
* 0   console    admin           0:00:00
  1     vty 0    admin           0:04:37      10.1.0.19

Console#
```

show version

This command displays hardware and software version information for the system.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Downloaded from www.Manualslib.com manuals search engine

Command Usage

See "Displaying Switch Hardware/Software Versions" on page 3-16 for detailed information on the items displayed by this command.

Example

```
Console#show version
Unit1
 Serial number           : A322043872
 Hardware version        : R01
 Number of ports         :12
 Main power status       :up
 Redundant power status  :down
Agent (master)
 Unit ID                 : 1
 Loader version          : 2.0.2.3
 Boot ROM version        : 2.0.2.1
 Operation code version  : 2.2.3.2
Console#
```

Frame Size Commands

Command	Function	Mode	Page
jumbo frame	Enables support for jumbo frames	GC	3-84

jumbo frame

This command enables support for jumbo frames. Use the **no** form to disable it.

Syntax

[**no**] **jumbo frame**

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- This switch provides more efficient throughput for large sequential data transfers by supporting jumbo frames up to 9216 bytes. Compared

Downloaded from www.Manualslib.com manuals search engine

to standard Ethernet frames that run only up to 1.5 KB, using jumbo frames significantly reduces the per-packet overhead required to process protocol encapsulation fields.

- To use jumbo frames, both the source and destination end nodes (such as a computer or server) must support this feature. Also, when the connection is operating at full duplex, all switches in the network between the two end nodes must be able to accept the extended frame size. And for half-duplex connections, all devices in the collision domain would need to support jumbo frames.
- Enabling jumbo frames will limit the maximum threshold for broadcast storm control to 64 packets per second. (See the **switchport broadcast** command on page 3-9.)

Example

```
Console(config)#jumbo frame
Console(config)#
```

Flash/File Commands

These commands are used to manage the system code or configuration files.

Command	Function	Mode	Page
copy	Copies a code image or a switch configuration to or from flash memory or a TFTP server	PE	3-85
delete	Deletes a file or code image	PE	3-88
dir	Displays a list of files in flash memory	PE	3-89
whichboot	Displays the files booted	PE	3-90
boot system	Specifies the file or image used to start up the system	GC	3-91

copy

This command moves (upload/download) a code image or configuration file between the switch's flash memory and a TFTP server. When you save the system code or configuration settings to a file on a TFTP server, that file can later be downloaded to the switch to restore system operation. The

Downloaded from www.Manualslib.com manuals search engine

success of the file transfer depends on the accessibility of the TFTP server and the quality of the network connection.

Syntax

copy file {**file** | **running-config** | **startup-config** | **tftp**}
copy running-config {**file** | **startup-config** | **tftp**}
copy startup-config {**file** | **running-config** | **tftp**}
copy tftp {**file** | **running-config** | **startup-config** | **https-certificate**}

- **file** - Keyword that allows you to copy to/from a file.
- **running-config** - Keyword that allows you to copy to/from the current running configuration.
- **startup-config** - The configuration used for system initialization.
- **tftp** - Keyword that allows you to copy to/from a TFTP server.
- **https-certificate** - Copies an HTTPS certificate from an TFTP server to the switch.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- The system prompts for data required to complete the copy command.
- The destination file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names on the TFTP server is 127 characters or 31 characters for files on the switch. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")
- Due to the size limit of the flash memory, the switch supports only two operation code files.
- The maximum number of user-defined configuration files depends on available memory.
- You can use "Factory_Default_Config.cfg" as the source to copy from

Downloaded from www.Manualslib.com manuals search engine

the factory default configuration file, but you cannot use it as the destination.

- To replace the startup configuration, you must use **startup-config** as the destination.
- The Boot ROM and Loader cannot be uploaded or downloaded from the TFTP server. You must use a direct console connection and access the download menu during a boot up to download the Boot ROM (or diagnostic) image. See "Upgrading Firmware via the Serial Port" on page B-1 for more details.

Example

The following example shows how to upload the configuration settings to a file on the TFTP server:

```
Console#copy file tftp
Choose file type:
 1. config:  2. opcode: <1-2>: 1
Source file name: startup
TFTP server ip address: 10.1.0.99
Destination file name: startup.01
TFTP completed.
Success.

Console#
```

The following example shows how to copy the running configuration to a startup file.

```
Console#copy running-config file
destination file name: startup
Write to FLASH Programming.
\Write to FLASH finish.
Success.

Console#
```


Downloaded from www.Manualslib.com manuals search engine

The following example shows how to download a configuration file:

```
Console#copy tftp startup-config
TFTP server ip address: 10.1.0.99
Source configuration file name: startup.01
Startup configuration file name [startup]:
Write to FLASH Programming.

\Write to FLASH finish.
Success.

Console#
```

This example shows how to copy a secure-site certificate from an TFTP server. It then reboots the switch to activate the certificate:

```
Console#copy tftp https-certificate
TFTP server ip address: 10.1.0.19
Source certificate file name: SS-certificate
Source private file name: SS-private
Private password: ********

Success.
Console#reload
System will be restarted, continue <y/n>? y
```

delete

This command deletes a file or image.

Syntax

delete *filename*

filename - Name of the configuration file or image name.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- If the file type is used for system startup, then this file cannot be deleted.

Downloaded from www.Manualslib.com manuals search engine

- "Factory_Default_Config.cfg" cannot be deleted.

Example

This example shows how to delete the test2.cfg configuration file from flash memory.

```
Console#delete test2.cfg
Console#
```

Related Commands

dir (3-89)

dir

This command displays a list of files in flash memory.

Syntax

dir [**boot-rom** | **config** | **opcode** [:*filename*]]

The type of file or image to display includes:

- **boot-rom** - Boot ROM (or diagnostic) image file.
- **config** - Switch configuration file.
- **opcode** - Run-time operation code image file.
- *filename* - Name of the file or image. If this file exists but contains errors, information on this file cannot be shown.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- If you enter the command **dir** without any parameters, the system displays all files.

Downloaded from www.Manualslib.com manuals search engine

- File information is shown below:

Column Heading	Description
file name	The name of the file.
file type	File types: Boot-Rom, Operation Code, and Config file.
startup	Shows if this file is used when the system is started.
size	The length of the file in bytes.

Example

The following example shows how to display all file information:

```
Console#dir
                        file name      file type startup size (byte)
------------------------------ -------------- ------- -----------
                        diag_0060 Boot-Rom image       Y      111360
                        run_01642 Operation Code       N     1074304
                         run_0200 Operation Code       Y     1083008
      Factory_Default_Config.cfg    Config File       N        2574
                          startup    Config File       Y        2710
-----------------------------------------------------------------
                                       Total free space:         0
Console#
```

whichboot

This command displays which files were booted when the system powered up.

Default Setting

None

Command Mode

Privileged Exec

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows the information displayed by the **whichboot** command. See the table under the **dir** command for a description of the file information displayed by this command.

```
Console#whichboot
        file name      file type startup size (byte)
----------------- -------------- ------- -----------
        diag_0060 Boot-Rom image       Y      111360
         run_0200 Operation Code       Y     1083008
          startup    Config File       Y        2710
Console#
```

boot system

This command specifies the file or image used to start up the system.

Syntax

boot system {**boot-rom**| **config** | **opcode**}: *filename*

The type of file or image to set as a default includes:

- **boot-rom** - Boot ROM.
- **config** - Configuration file.
- **opcode** - Run-time operation code.

The colon (:) is required.

filename - Name of the configuration file or image name.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- A colon (:) is required after the specified file type.
- If the file contains an error, it cannot be set as the default file.

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console(config)#boot system config: startup
Console(config)#
```

Related Commands

dir (3-89)
whichboot (3-90)

Authentication Commands

You can configure this switch to authenticate users logging into the system for management access using local or RADIUS authentication methods. You can also enable port-based authentication for network client access using IEEE 802.1x.

Command Group	Function	Page
Authentication Sequence	Defines logon authentication method and precedence	3-93
RADIUS Client	Configures settings for authentication via a RADIUS server	3-94
TACACS+ Client	Configures settings for authentication via a TACACS+ server	3-98
Port Security	Configures secure addresses for a port	3-101
Port Authentication	Configures host authentication on specific ports using 802.1x	3-104

Downloaded from www.Manualslib.com manuals search engine

Authentication Sequence

Command	Function	Mode	Page
authentication login	Defines logon authentication method and precedence	GC	3-93

authentication login

This command defines the login authentication method and precedence. Use the **no** form to restore the default.

Syntax

authentication login {[**local**] [**radius**] [**tacacs**]}
no authentication login

- **local** - Use local password.
- **radius** - Use RADIUS server password.
- **tacacs** - Use TACACS server password.

Default Setting

Local

Command Mode

Global Configuration

Command Usage

- RADIUS uses UDP while TACACS+ uses TCP. UDP only offers best effort delivery, while TCP offers a connection-oriented transport. Also, note that RADIUS encrypts only the password in the access-request packet from the client to the server, while TACACS+ encrypts the entire body of the packet.
- RADIUS and TACACS+ logon authentication assigns a specific privilege level for each user name and password pair. The user name, password, and privilege level must be configured on the authentication server.
- You can specify three authentication methods in a single command to indicate the authentication sequence. For example, if you enter "**authentication login radius tacacs local**," the user name and

Downloaded from www.Manualslib.com manuals search engine

password on the RADIUS server is verified first. If the RADIUS server is not available, then authentication is attempted on the TACACS+ server. If the TACACS+ server is not available, the local user name and password is checked.

Example

```
Console(config)#authentication login radius
Console(config)#
```

Related Commands

username - for setting the local user names and passwords (3-35)

RADIUS Client

Remote Authentication Dial-in User Service (RADIUS) is a logon authentication protocol that uses software running on a central server to control access to RADIUS-aware devices on the network. An authentication server contains a database of multiple user name/password pairs with associated privilege levels for each user or group that require management access to a switch.

Command	Function	Mode	Page
radius-server host	Specifies the RADIUS server	GC	3-95
radius-server port	Sets the RADIUS server network port	GC	3-95
radius-server key	Sets the RADIUS encryption key	GC	3-96
radius-server retransmit	Sets the number of retries	GC	3-96
radius-server timeout	Sets the interval between sending authentication requests	GC	3-97
show radius-server	Shows the current RADIUS settings	PE	3-97

Downloaded from www.Manualslib.com manuals search engine

radius-server host

This command specifies the RADIUS server. Use the **no** form to restore the default.

Syntax

radius-server host *host_ip_address*
no radius-server host

host_ip_address - IP address of server.

Default Setting

10.1.0.1

Command Mode

Global Configuration

Example

```
Console(config)#radius-server host 192.168.1.25
Console(config)#
```

radius-server port

This command sets the RADIUS server network port. Use the **no** form to restore the default.

Syntax

radius-server port *port_number*
no radius-server port

port_number - RADIUS server UDP port used for authentication messages. (Range: 1-65535)

Default Setting

1812

Command Mode

Global Configuration

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console(config)#radius-server port 181
Console(config)#
```

radius-server key

This command sets the RADIUS encryption key. Use the **no** form to restore the default.

Syntax

radius-server key *key_string*
no radius-server key

key_string - Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 20 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#radius-server key green
Console(config)#
```

radius-server retransmit

This command sets the number of retries. Use the **no** form to restore the default.

Syntax

radius-server retransmit *number_of_retries*
no radius-server retransmit

number_of_retries - Number of times the switch will try to authenticate logon access via the RADIUS server. (Range: 1 - 30)

Downloaded from www.Manualslib.com manuals search engine

Default Setting

2

Command Mode

Global Configuration

Example

```
Console(config)#radius-server retransmit 5
Console(config)#
```

radius-server timeout

This command sets the interval between transmitting authentication requests to the RADIUS server. Use the **no** form to restore the default.

Syntax

radius-server timeout *number_of_seconds*
no radius-server timeout

number_of_seconds - Number of seconds the switch waits for a reply before resending a request. (Range: 1-65535)

Default Setting

5

Command Mode

Global Configuration

Example

```
Console(config)#radius-server timeout 10
Console(config)#
```

show radius-server

This command displays the current settings for the RADIUS server.

Default Setting

None

Downloaded from www.Manualslib.com manuals search engine

Command Mode

Privileged Exec

Example

```
Console#show radius-server
Server IP address: 10.1.0.1
 Communication key with radius server:
 Server port number: 1812
 Retransmit times: 2
 Request timeout: 5
Console#
```

TACACS+ Client

Terminal Access Controller Access Control System (TACACS+) is a logon authentication protocol that uses software running on a central server to control access to TACACS-aware devices on the network. An authentication server contains a database of multiple user name/password pairs with associated privilege levels for each user or group that require management access to a switch.

Command	Function	Mode	Page
tacacs-server host	Specifies the TACACS+ server	GC	3-98
tacacs-server port	Specifies the TACACS+ server network port	GC	3-99
tacacs-server key	Sets the TACACS+ encryption key	GC	3-99
show tacacs-server	Shows the current TACACS+ settings	GC	3-100

tacacs-server host

This command specifies the TACACS+ server. Use the **no** form to restore the default.

Syntax

tacacs-server host *host_ip_address*
no tacacs-server host

host_ip_address - IP address of a TACACS+ server.

Downloaded from www.Manualslib.com manuals search engine

Default Setting

10.11.12.13

Command Mode

Global Configuration

Example

```
Console(config)#tacacs-server host 192.168.1.25
Console(config)#
```

tacacs-server port

This command specifies the TACACS+ server network port. Use the **no** form to restore the default.

Syntax

tacacs-server port *port_number*
no tacacs-server port

port_number - TACACS+ server TCP port used for authentication messages. (Range: 1-65535)

Default Setting

49

Command Mode

Global Configuration

Example

```
Console(config)#tacacs-server port 181
Console(config)#
```

tacacs-server key

This command sets the TACACS+ encryption key. Use the **no** form to restore the default.

Downloaded from www.Manualslib.com manuals search engine

Syntax

tacacs-server key *key_string*
no tacacs-server key

key_string - Encryption key used to authenticate logon access for the client. Do not use blank spaces in the string.
(Maximum length: 20 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#tacacs-server key green
Console(config)#
```

show tacacs-server

This command displays the current settings for the TACACS+ server.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show tacacs-server
Remote TACACS server configuration:
 Server IP address: 10.11.12.13
 Communication key with radius server: green
 Server port number: 49
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Port Security Commands

These commands can be used to disable the learning function or manually specify secure addresses for a port. You may want to leave port security off for an initial training period (i.e., enable the learning function) to register all the current VLAN members on the selected port, and then enable port security to ensure that the port will drop any incoming frames with a source MAC address that is unknown or has been previously learned from another port.

Command	Function	Mode	Page
port security	Configures a secure port	IC	3-101
mac-address-table static	Maps a static address to a port in a VLAN	GC	3-34
show mac-address-table	Displays entries in the bridge-forwarding database	PE	3-35

port security

This command enables or configures port security. Use the **no** form without any keywords to disable port security. Use the **no** form with the appropriate keyword to restore the default settings for a response to security violation or for the maximum number of allowed addresses.

Syntax

port security [**action** {**shutdown** | **trap** | **trap-and-shutdown**} | **max-mac-count** *address-count*]
no port security [**action** | **max-mac-count**]

- **action** - Response to take when port security is violated.
  - **shutdown** - Disable port only.
  - **trap** - Issue SNMP trap message only.
  - **trap-and-shutdown** - Issue SNMP trap message and disable port.
- **max-mac-count**
  - *address-count* - The maximum number of MAC addresses that can be learned on a port. (Range: 0 - 20)

Downloaded from www.Manualslib.com manuals search engine

Default Setting

Status: Disabled
Action: None
Maximum Addresses: 0

Command Mode

Interface Configuration (Ethernet)

Command Usage

- If you enable port security, the switch will stop dynamically learning new addresses on the specified port. Only incoming traffic with source addresses already stored in the dynamic or static address table will be accepted.
- To use port security, first allow the switch to dynamically learn the <source MAC address, VLAN> pair for frames received on a port for an initial training period, and then enable port security to stop address learning. Be sure you enable the learning function long enough to ensure that all valid VLAN members have been registered on the selected port.
- To add new VLAN members at a later time, you can manually add secure addresses with the **mac-address-table static** command, or turn off port security to re-enable the learning function long enough for new VLAN members to be registered. Learning may then be disabled again, if desired, for security.
- A secure port has the following restrictions:
  - Cannot use port monitoring.
  - Cannot be a multi-VLAN port.
  - Cannot be connected to a network interconnection device.
  - Cannot be a trunk port.
- If a port is disabled due to a security violation, it must be manually re-enabled using the **no shutdown** command.

Downloaded from www.Manualslib.com manuals search engine

Example

The following example enables port security for port 5, and sets the response to a security violation to issue a trap message:

```
Console(config)#interface ethernet 1/5
Console(config-if)#port security action trap
```

Related Commands

shutdown (3-9)
mac-address-table static (3-34)
show mac-address-table (3-35)

Downloaded from www.Manualslib.com manuals search engine

802.1x Port Authentication

The switch supports IEEE 802.1x (dot1x) port-based access control that prevents unauthorized access to the network by requiring users to first submit credentials for authentication. Client authentication is controlled centrally by a RADIUS server using EAP (Extensible Authentication Protocol).

Command	Function	Mode	Page
authentication dot1x default	Sets the default authentication server type	GC	3-104
dot1x default	Resets all dot1x parameters to their default values	GC	3-105
dot1x max-req	Sets the maximum number of times that the switch retransmits an EAP request/identity packet to the client before it times out the authentication session	GC	3-105
dot1x port-control	Sets dot1x mode for a port interface	IC	3-106
dot1x operation-mode	Allows single or multiple hosts on an dot1x port	IC	3-107
dot1x re-authenticate	Forces re-authentication on specific ports	PE	3-107
dot1x re-authentication	Enables re-authentication for all ports	GC	3-108
dot1x timeout quiet-period	Sets the time that a switch port waits after the Max Request Count has been exceeded before attempting to acquire a new client	GC	3-108
dot1x timeout re-authperiod	Sets the time period after which a connected client must be re-authenticated	GC	3-109
dot1x timeout tx-period	Sets the time period during an authentication session that the switch waits before re-transmitting an EAP packet	GC	3-109
show dot1x	Shows all dot1x related information	PE	3-110

authentication dot1x default

This command sets the default authentication server type. Use the **no** form to restore the default.

Downloaded from www.Manualslib.com manuals search engine

Syntax

authentication dot1x default radius
no authentication dot1x

Default Setting

RADIUS

Command Mode

Global Configuration

Example

```
Console(config)#authentication dot1x default radius
Console(config)#
```

dot1x default

This command sets all configurable dot1x global and port settings to their default values.

Syntax

dot1x default

Command Mode

Global Configuration

Example

```
Console(config)#dot1x default
Console(config)#
```

dot1x max-req

This command sets the maximum number of times the switch port will retransmit an EAP request/identity packet to the client before it times out the authentication session. Use the **no** form to restore the default.

Syntax

dot1x max-req *count*
no dot1x max-req

Downloaded from www.Manualslib.com manuals search engine

count – The maximum number of requests (Range: 1-10)

Default

2

Command Mode

Global Configuration

Example

```
Console(config)#dot1x max-req 2
Console(config)#
```

dot1x port-control

This command sets the dot1x mode on a port interface. Use the **no** form to restore the default.

Syntax

dot1x port-control {**auto** | **force-authorized** | **force-unauthorized**}
no dot1x port-control

- **auto** – Requires a dot1x-aware connected client to be authorized by the RADIUS server. Clients that are not dot1x-aware will be denied access.
- **force-authorized** – Configures the port to grant access to all clients, either dot1x-aware or otherwise.
- **force-unauthorized** – Configures the port to deny access to all clients, either dot1x-aware or otherwise.

Default

force-authorized

Command Mode

Interface Configuration

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x port-control auto
Console(config-if)#
```


Downloaded from www.Manualslib.com manuals search engine

dot1x operation-mode

This command allows single or multiple hosts (clients) to connect to an 802.1X-authorized port. Use the **no** form with no keywords to restore the default to single host. Use the **no** form with the **multi-host max-count** keywords to restore the default maximum count.

Syntax

dot1x operation-mode {**single-host** | **multi-host** [**max-count** *count*]}
no dot1x operation-mode [**multi-host max-count**]

- **single-host** – Allows only a single host to connect to this port.
- **multi-host** – Allows multiple host to connect to this port.
- **max-count** – Keyword for the maximum number of hosts.
  - *count* – The maximum number of hosts that can connect to a port. (Range: 1-20; Default: 5)

Default

Single-host

Command Mode

Interface Configuration

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x operation-mode multi-host max-count 10
Console(config-if)#
```

dot1x re-authenticate

This command forces re-authentication on all ports or a specific interface.

Syntax

dot1x re-authenticate [*interface*]

interface

- **ethernet** *unit/port*

Downloaded from www.Manualslib.com manuals search engine

- *unit* - This is device 1.
- *port* - Port number.

Command Mode

Privileged Exec

Example

```
Console#dot1x re-authenticate
Console#
```

dot1x re-authentication

This command enables periodic re-authentication globally for all ports. Use the **no** form to disable re-authentication.

Syntax

[**no**] **dot1x re-authentication**

Command Mode

Global Configuration

Example

```
Console(config)#dot1x re-authentication
Console(config)#
```

dot1x timeout quiet-period

This command sets the time that a switch port waits after the Max Request Count has been exceeded before attempting to acquire a new client. Use the **no** form to reset the default.

Syntax

dot1x timeout quiet-period *seconds*
no dot1x timeout quiet-period

seconds - The number of seconds. (Range: 1-65535)

Default

60 seconds

Downloaded from www.Manualslib.com manuals search engine

Command Mode

Global Configuration

Example

```
Console(config)#dot1x timeout quiet-period 350
Console(config)#
```

dot1x timeout re-authperiod

This command sets the time period after which a connected client must be re-authenticated.

Syntax

dot1x timeout re-authperiod *seconds*
no dot1x timeout re-authperiod

seconds - The number of seconds. (Range: 1-65535)

Default

3600 seconds

Command Mode

Global Configuration

Example

```
Console(config)#dot1x timeout re-authperiod 300
Console(config)#
```

dot1x timeout tx-period

This command sets the time that the switch waits during an authentication session before re-transmitting an EAP packet. Use the **no** form to reset to the default value.

Syntax

dot1x timeout tx-period *seconds*
no dot1x timeout tx-period

seconds - The number of seconds. (Range: 1-65535)

Downloaded from www.Manualslib.com manuals search engine

Default

30 seconds

Command Mode

Global Configuration

Example

```
Console(config)#dot1x timeout tx-period 300
Console(config)#
```

show dot1x

This command shows general port authentication related settings on the switch or a specific interface.

Syntax

show dot1x [**statistics**] [**interface** *interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - This is device 1.
  - *port* - Port number.

Command Mode

Privileged Exec

Command Usage

This command displays the following information:

- *Global 802.1X Parameters* – Displays the global port access control parameters that can be configured for this switch as described in the preceding pages, including reauth-enabled (page 3-108), reauth-period (page 3-109), quiet-period (page 3-108), tx-period (page 3-109), and max-req (page 3-105). It also displays the

Downloaded from www.Manualslib.com manuals search engine

following global parameters which are set to a fixed value, including the following items:

- supp-timeout – Supplicant timeout.
- server-timeout– Server timeout.
- reauth-max – Maximum number of reauthentication attempts.

- *802.1X Port Summary* – Displays the port access control parameters for each interface, including the following items:
  - Status – Administrative state for port access control.
  - Mode – Dot1x port control mode (page 3-106).
  - Authorized – Authorization status (yes or n/a - not authorized).
- *802.1X Port Details* – Displays detailed port access control settings for each interface as described in the preceding pages, including administrative status for port access control, Max request (page 3-105), Quiet period (page 3-108), Reauth period (page 3-109), Tx period (page 3-109), and Port-control (page 3-106). It also displays the following information:
  - Status – Authorization status (authorized or unauthorized).
  - Supplicant – MAC address of authorized client.
- *Authenticator State Machine*
  - State – Current state (including initialize, disconnected, connecting, authenticating, authenticated, aborting, held, force_authorized, force_unauthorized).
  - Reauth Count– Number of times connecting state is re-entered.
- *Backend State Machine*
  - State – Current state (including request, response, success, fail, timeout, idle, initialize).
  - Request Count– Number of EAP Request packets sent to the Supplicant without receiving a response.
  - Identifier(Server)– Identifier carried in the most recent EAP Success, Failure or Request packet received from the Authentication Server.
- *Reauthentication State Machine*

Downloaded from www.Manualslib.com manuals search engine

- State – Current state (including initialize, reauthenticate).

Example

```
Console#show dot1x
Global 802.1X Parameters
 reauth-enabled: no
 reauth-period:  3600
 quiet-period:   60
 tx-period:      30
 supp-timeout:   30
 server-timeout: 10
 reauth-max:     2
 max-req:        2
802.1X Port Summary
 Port Name     Status           Mode          Authorized
         1       disabled    ForceAuthorized           n/a
         2       disabled    ForceAuthorized           n/a
.
.
.
        11       disabled    ForceAuthorized           yes
        12        enabled               Auto           yes

802.1X Port Details

802.1X is disabled on port 1
.
.
.
802.1X is enabled on port 12
Max request         2
Quiet period        350
Reauth period       300
Tx period           300
Status              Unauthorized
Port-control        Auto
Supplicant          00-00-00-00-00-00

Authenticator State Machine
State               Connecting
Reauth Count        3
Backend State Machine
State               Idle
Request Count       0
Identifier(Server)  0

Reauthentication State Machine
State               Initialize
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Access Control List Commands

Access Control Lists (ACL) provide packet filtering for IP frames (based on address, protocol, Layer 4 protocol port number or TCP control code) or any frames (based on MAC address or Ethernet type). To filter packets, first create an access list, add the required rules, specify a mask to modify the precedence in which the rules are checked, and then bind the list to a specific port.

Access Control Lists

An ACL is a sequential list of permit or deny conditions that apply to IP addresses, MAC addresses, or other more specific criteria. This switch tests ingress or egress packets against the conditions in an ACL one by one. A packet will be accepted as soon as it matches a permit rule, or dropped as soon as it matches a deny rule. If no rules match for a list of all permit rules, the packet is dropped; and if no rules match for a list of all deny rules, the packet is accepted.

There are three filtering modes:

- Standard IP ACL mode (STD-ACL) filters packets based on the source IP address.
- Extended IP ACL mode (EXT-ACL) filters packets based on source or destination IP address, as well as protocol type and protocol port number. If the TCP protocol is specified, then you can also filter packets based on the TCP control code.
- MAC ACL mode (MAC-ACL) filters packets based on the source or destination MAC address and the Ethernet frame type (RFC 1060).

The following restrictions apply to ACLs:

- This switch supports ACLs for both ingress and egress filtering. However, you can only bind one IP ACL and one MAC ACL to any port for ingress filtering, and one IP ACL and one MAC ACL to any port for egress filtering. In other words, only four ACLs can be bound

Downloaded from www.Manualslib.com manuals search engine

to an interface – Ingress IP ACL, Egress IP ACL, Ingress MAC ACL and Egress MAC ACL.

- When an ACL is bound to an interface as an egress filter, all entries in the ACL must be deny rules. Otherwise, the bind operation will fail.
- Each ACL can have up to 32 rules.
- The maximum number of ACLs is also 32.
- However, due to resource restrictions, the average number of rules bound the ports should not exceed 20.
- You must configure a mask for an ACL rule before you can bind it to a port or set the queue or frame priorities associated with the rule.
- The switch does not support the explicit "deny any any" rule for the egress IP ACL or the egress MAC ACLs. If these rules are included in ACL, and you attempt to bind the ACL to an interface for egress checking, the bind operation will fail.
- Egress MAC ACLs only work for destination-mac-known packets, not for multicast, broadcast, or destination-mac-unknown packets.

The order in which active ACLs are checked is as follows:

1.User-defined rules in the Egress MAC ACL for egress ports.

2.User-defined rules in the Egress IP ACL for egress ports.

3.User-defined rules in the Ingress MAC ACL for ingress ports.

4.User-defined rules in the Ingress IP ACL for ingress ports.

5.Explicit default rule (permit any any) in the ingress IP ACL for ingress ports.

6.Explicit default rule (permit any any) in the ingress MAC ACL for ingress ports.

7.If no explicit rule is matched, the implicit default is permit all.

Masks for Access Control Lists

You can specify optional masks that control the order in which ACL rules are checked. The switch includes two system default masks that pass/filter packets matching the permit/deny the rules specified in an ingress ACL. You can also configure up to seven user-defined masks for an ACL. A mask must be bound exclusively to one of the basic ACL types (i.e., Ingress

Downloaded from www.Manualslib.com manuals search engine

IP ACL, Egress IP ACL, Ingress MAC ACL or Egress MAC ACL), but a mask can be bound to up to four ACLs of the same type.

Command Groups	Function	Page
IP ACLs	Configures ACLs based on IP addresses, TCP/UDP port number, protocol type, and TCP control code	3-115
MAC ACLs	Configures ACLs based on hardware addresses, packet format, and Ethernet type	3-133
ACL Information	Displays ACLs and associated rules; shows ACLs assigned to each port	3-146

IP ACLs

Command	Function	Mode	Page
access-list ip	Creates an IP ACL and enters configuration mode	GC	3-116
permit, deny	Filters packets matching a specified source IP address	STD-ACL	3-117
permit, deny	Filters packets meeting the specified criteria, including source and destination IP address, TCP/UDP port number, protocol type, and TCP control code	EXT-ACL	3-118
show ip access-list	Displays the rules for configured IP ACLs	PE	3-121
access-list ip mask-precedence	Changes to the mode for configuring access control masks	GC	3-121
mask	Sets a precedence mask for the ACL rules	IP-Mask	3-122
show access-list ip mask-precedence	Shows the ingress or egress rule masks for IP ACLs	PE	3-126
ip access-group	Adds a port to an IP ACL	IC	3-127
show ip access-group	Shows port assignments for IP ACLs	PE	3-127
map access-list ip	Sets the CoS value and corresponding output queue for packets matching an ACL rule	IC	3-128

Downloaded from www.Manualslib.com manuals search engine

Command	Function	Mode	Page
show map access-list ip	Shows CoS value mapped to an access list for an interface	PE	3-129
match access-list ip	Changes the 802.1p priority, IP Precedence, or DSCP Priority of a frame matching the defined rule (i.e., also called packet marking)	IC	3-130
show marking	Displays the current configuration for packet marking	PE	3-131

access-list ip

This command adds an IP access list and enters configuration mode for standard or extended IP ACLs. Use the **no** form to remove the specified ACL.

Syntax

[**no**] **access-list ip** {**standard** | **extended**} *acl_name*

- **standard** – Specifies an ACL that filters packets based on the source IP address.
- **extended** – Specifies an ACL that filters packets based on the source or destination IP address, and other more specific criteria.
- *acl_name* – Name of the ACL. (Maximum length: 16 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- An egress ACL must contain all deny rules.
- When you create a new ACL or enter configuration mode for an existing ACL, use the **permit** or **deny** command to add new rules to the bottom of the list. To create an ACL, you must add at least one rule to the list.

Downloaded from www.Manualslib.com manuals search engine

- To remove a rule, use the **no permit** or **no deny** command followed by the exact text of a previously configured rule.
- An ACL can contain up to 32 rules.

Example

```
Console(config)#access-list ip standard david
Console(config-std-acl)#
```

Related Commands

permit, deny 3-117
ip access-group (3-127)
show ip access-list (3-121)

permit, **deny** (Standard ACL)

This command adds a rule to a Standard IP ACL. The rule sets a filter condition for packets emanating from the specified source. Use the **no** form to remove a rule.

Syntax

[**no**] {**permit | deny**} {**any** | *source bitmask* | **host** *source*}

- **any** – Any source IP address.
- *source* – Source IP address.
- *bitmask* – Decimal number representing the address bits to match.
- **host** – Keyword followed by a specific IP address.

Default Setting

None

Command Mode

Standard ACL

Command Usage

- New rules are appended to the end of the list.
- Address bitmasks are similar to a subnet mask, containing four integers from 0 to 255, each separated by a period. The binary mask uses 1 bits

Downloaded from www.Manualslib.com manuals search engine

to indicate "match" and 0 bits to indicate "ignore." The bitmask is bitwise ANDed with the specified source IP address, and then compared with the address for each IP packet entering the port(s) to which this ACL has been assigned.

Example

This example configures one permit rule for the specific address 10.1.1.21 and another rule for the address range 168.92.16.x – 168.92.31.x using a bitmask.

```
Console(config-std-acl)#permit host 10.1.1.21
Console(config-std-acl)#permit 168.92.16.0 255.255.240.0
Console(config-std-acl)#
```

Related Commands

access-list ip (3-116)

permit, **deny** (Extended ACL)

This command adds a rule to an Extended IP ACL. The rule sets a filter condition for packets with specific source or destination IP addresses, protocol types, source or destination protocol ports, or TCP control codes. Use the **no** form to remove a rule.

Syntax

[**no**] {**permit** | **deny**} [*protocol-number* | **udp**]
{**any** | *source address-bitmask* | **host** *source*}
{**any** | *destination address-bitmask* | **host** *destination*}
[**precedence** *precedence*] [**tos** *tos*] [**dscp** *dscp*]
[**source-port** *sport* [*bitmask*]] [**destination-port** *dport* [*port-bitmask*]]

[**no**] {**permit** | **deny**} **tcp**
{**any** | *source address-bitmask* | **host** *source*}
{**any** | *destination address-bitmask* | **host** *destination*}
[**precedence** *precedence*] [**tos** *tos*] [**dscp** *dscp*]
[**source-port** *sport* [*bitmask*]] [**destination-port** *dport* [*port-bitmask*]]
[**control-flag** *control-flags flag-bitmask*]

Downloaded from www.Manualslib.com manuals search engine

- *protocol-number* – A specific protocol number. (Range: 0-255)
- *source* – Source IP address.
- *destination* – Destination IP address.
- *address-bitmask* – Decimal number representing the address bits to match.
- **host** – Keyword followed by a specific IP address.
- *precedence* – IP precedence level. (Range: 0-7)
- *tos* – Type of Service level. (Range: 0-15)
- *dscp* – DSCP priority level. (Range: 0-64)
- *sport* – Protocol* source port number. (Range: 0-65535)
- *dport* – Protocol* destination port number. (Range: 0-65535)
- *port-bitmask* – Decimal number representing the port bits to match. (Range: 0-65535)
- *control-flags* – Decimal number (representing a bit string) that specifies flag bits in byte 14 of the TCP header. (Range: 0-63)
- *flag-bitmask* – Decimal number representing the code bits to match.

* Includes TCP, UDP or other protocol types.

Default Setting

None

Command Mode

Extended ACL

Command Usage

- All new rules are appended to the end of the list.
- Address bitmasks are similar to a subnet mask, containing four integers from 0 to 255, each separated by a period. The binary mask uses 1 bits to indicate "match" and 0 bits to indicate "ignore." The bitmask is bitwise ANDed with the specified source IP address, and then compared with the address for each IP packet entering the port(s) to which this ACL has been assigned.
- You can specify both Precedence and ToS in the same rule. However, if DSCP is used, then neither Precedence nor ToS can be specified.

Downloaded from www.Manualslib.com manuals search engine

- The control-code bitmask is a decimal number (representing an equivalent bit mask) that is applied to the control code. Enter a decimal number, where the equivalent binary bit "1" means to match a bit and "0" means to ignore a bit. The following bits may be specified:

- 1 (fin) – Finish
- 2 (syn) – Synchronize
- 4 (rst) – Reset
- 8 (psh) – Push
- 16 (ack) – Acknowledgement
- 32 (urg) – Urgent pointer

For example, use the code value and mask below to catch packets with the following flags set:

- SYN flag valid, use "control-code 2 2"
- Both SYN and ACK valid, use "control-code 18 18"
- SYN valid and ACK invalid, use "control-code 2 18"

Example

This example accepts any incoming packets if the source address is within subnet 10.7.1.x. For example, if the rule is matched; i.e., the rule (10.7.1.0 & 255.255.255.0) equals the masked address (10.7.1.2 & 255.255.255.0), the packet passes through.

```
Console(config-ext-acl)#permit 10.7.1.1 255.255.255.0 any
Console(config-ext-acl)#
```

This allows TCP packets from class C addresses 192.168.1.0 to any destination address when set for destination TCP port 80 (i.e., HTTP).

```
Console(config-ext-acl)#permit 192.168.1.0 255.255.255.0 any dport 80
Console(config-ext-acl)#
```


Downloaded from www.Manualslib.com manuals search engine

This permits all TCP packets from class C addresses 192.168.1.0 with the TCP control code set to "SYN."

```
Console(config-ext-acl)#permit 192.168.1.0 255.255.255.0 any tcp
control-code 2 2
Console(config-ext-acl)#
```

Related Commands

access-list ip (3-116)

show ip access-list

This command displays the rules for configured IP ACLs.

Syntax

show ip access-list {**standard** | **extended**} [*acl_name*]

- **standard** – Specifies a standard IP ACL.
- **extended** – Specifies an extended IP ACL.
- *acl_name* – Name of the ACL. (Maximum length: 16 characters)

Command Mode

Privileged Exec

Example

```
Console#show ip access-list standard
IP standard access-list david:
  permit host 10.1.1.21
  permit 168.92.0.0 0.0.15.255
Console#
```

Related Commands

permit, deny 3-117
ip access-group (3-127)

access-list ip mask-precedence

This command changes to the IP Mask mode used to configure access control masks. Use the **no** form to delete the mask table.

Downloaded from www.Manualslib.com manuals search engine

Syntax

[**no**] **access-list ip mask-precedence** {**in** | **out**}

- **in** – Ingress mask for ingress ACLs.
- **out** – Egress mask for egress ACLs.

Default Setting

Default system mask: Filter inbound packets according to specified IP ACLs.

Command Mode

Global Configuration

Command Usage

- A mask can only be used by all ingress ACLs or all egress ACLs.
- The precedence of the ACL rules applied to a packet is not determined by order of the rules, but instead by the order of the masks; i.e., the first mask that matches a rule will determine the rule that is applied to a packet.
- You must configure a mask for an ACL rule before you can bind it to a port or set the queue or frame priorities associated with the rule.

Example

```
Console(config)#access-list ip mask-precedence in
Console(config-ip-mask-acl)#
```

Related Commands

mask (IP ACL) (3-122)
ip access-group (3-127)

mask (IP ACL)

This command defines a mask for IP ACLs. This mask defines the fields to check in the IP header. Use the **no** form to remove a mask.

Downloaded from www.Manualslib.com manuals search engine

Syntax

[**no**] **mask** [**protocol**]
{**any** | **host** | *source-bitmask*}
{**any** | **host** | *destination-bitmask*}
[**precedence**] [**tos**] [**dscp**]
[**source-port** [*port-bitmask*]] [**destination-port** [*port-bitmask*]]
[**control-flag** [*flag-bitmask*]]

- **protocol** – Check the protocol field.
- **any** – Any address will be matched.
- **host** – The address must be for a host device, not a subnetwork.
- *source-bitmask* – Source address of rule must match this bitmask.
- *destination-bitmask* – Destination address of rule must match this bitmask.
- **precedence** – Check the IP precedence field.
- **tos** – Check the TOS field.
- **dscp** – Check the DSCP field.
- **source-port** – Check the protocol source port field.
- **destination-port** – Check the protocol destination port field.
- *port-bitmask* – Protocol port of rule must match this bitmask. (Range: 0-65535)
- **control-flag** – Check the field for control flags.
- *flag-bitmask* – Control flags of rule must match this bitmask. (Range: 0-63)

Default Setting

None

Command Mode

IP Mask

Command Usage

- Packets crossing a port are checked against all the rules in the ACL until a match is found. The order in which these packets are checked is determined by the mask, and not the order in which the ACL rules were entered.

Downloaded from www.Manualslib.com manuals search engine

- First create the required ACLs and ingress or egress masks before mapping an ACL to an interface.
- If you enter **dscp**, you cannot enter **tos** or **precedence**. You can enter both **tos** and **precedence** without **dscp**.
- Masks that include an entry for a Layer 4 protocol source port or destination port can only be applied to packets with a header length of exactly five bytes.

Example

This example creates an IP ingress mask with two rules. Each rule is checked in order of precedence to look for a match in the ACL entries. The first entry matching a mask is applied to the inbound packet.

```
Console(config)#access-list ip mask-precedence in
Console(config-ip-mask-acl)#mask host any
Console(config-ip-mask-acl)#mask 255.255.255.0 any
Console(config-ip-mask-acl)#
```

This shows that the entries in the mask override the precedence in which the rules are entered into the ACL. In the following example, packets with the source address 10.1.1.1 are dropped because the "deny 10.1.1.1 255.255.255.255" rule has the higher precedence according the "mask host any" entry.

```
Console(config)#access-list ip standard A2
Console(config-std-acl)#permit 10.1.1.0 255.255.255.0
Console(config-std-acl)#deny 10.1.1.1 255.255.255.255
Console(config-std-acl)#exit
Console(config)#access-list ip mask-precedence in
Console(config-ip-mask-acl)#mask host any
Console(config-ip-mask-acl)#mask 255.255.255.0 any
Console(config-ip-mask-acl)#
```


Downloaded from www.Manualslib.com manuals search engine

This shows how to create a standard ACL with an ingress mask to deny access to the IP host 171.69.198.102, and permit access to any others.

```
Console(config)#access-list ip standard A2
Console(config-std-acl)#permit any
Console(config-std-acl)#deny host 171.69.198.102
Console(config-std-acl)#end
Console#show access-list
IP standard access-list A2:
  deny host 171.69.198.102
  permit any
Console#configure
Console(config)#access-list ip mask-precedence in
Console(config-ip-mask-acl)#mask host any
Console(config-ip-mask-acl)#exit
Console(config)#interface ethernet 1/1
Console(config-if)#ip access-group A2 in
Console(config-if)#end
Console#show access-list
IP standard access-list A2:
  deny host 171.69.198.102
  permit any
Console#
```

This shows how to create an extended ACL with an egress mask to drop packets leaving network 171.69.198.0 when the Layer 4 source port is 23.

```
Console(config)#access-list ip extended A3
Console(config-ext-acl)#deny host 171.69.198.5 any
Console(config-ext-acl)#deny 171.69.198.0 255.255.255.0 any source-port 23
Console(config-ext-acl)#end
Console#show access-list
IP extended access-list A3:
  deny host 171.69.198.5 any
  deny 171.69.198.0 255.255.255.0 any source-port 23
Console#config
Console(config)#access-list ip mask-precedence out
Console(config-ip-mask-acl)#mask 255.255.255.0 any source-port
Console(config-ip-mask-acl)#exit
Console(config)#interface ethernet 1/15
Console(config-if)#ip access-group A3 out
Console(config-if)#end
Console#show access-list
IP extended access-list A3:
  deny 171.69.198.0 255.255.255.0 any source-port 23
  deny host 171.69.198.5 any
IP egress mask ACL:
  mask 255.255.255.0 any source-port
Console#
```


Downloaded from www.Manualslib.com manuals search engine

This is a more comprehensive example. It denies any TCP packets in which the SYN bit is ON, and permits all other packets. It then sets the ingress mask to check the deny rule first, and finally binds port 1 to this ACL. Note that once the ACL is bound to an interface (i.e., the ACL is active), the order in which the rules are displayed is determined by the associated mask.

```
Switch(config)#access-list ip extended 6
Switch(config-ext-acl)#permit any any
Switch(config-ext-acl)#deny tcp any any control-flag 2 2
Switch(config-ext-acl)#end
Console#show access-list
IP extended access-list A6:
  permit any any
  deny tcp any any control-flag 2 2
Console#configure
Switch(config)#access-list ip mask-precedence in
Switch(config-ip-mask-acl)#mask protocol any any control-flag 2
Switch(config-ip-mask-acl)#end
Console#sh access-list
IP extended access-list A6:
  permit any any
  deny tcp any any control-flag 2 2
IP ingress mask ACL:
  mask protocol any any control-flag 2
Console#configure
Console(config)#interface ethernet 1/1
Console(config-if)#ip access-group A6 in
Console(config-if)#end
Console#show access-list
IP extended access-list A6:
  deny tcp any any control-flag 2 2
  permit any any
IP ingress mask ACL:
  mask protocol any any control-flag 2
Console#
```

show access-list ip mask-precedence

This command shows the ingress or egress rule masks for IP ACLs.

Syntax

show access-list ip mask-precedence [**in** | **out**]

- **in** – Ingress mask precedence for ingress ACLs.
- **out** – Egress mask precedence for egress ACLs.

Downloaded from www.Manualslib.com manuals search engine

Command Mode

Privileged Exec

Example

```
Console#show access-list ip mask-precedence
IP ingress mask ACL:
  mask host any
  mask 255.255.255.0 any
Console#
```

Related Commands

mask (IP ACL) (3-122)

ip access-group

This command binds a port to an IP ACL. Use the **no** form to remove the port.

Syntax

[**no**] **ip access-group** *acl_name* {**in** | **out**}

- *acl_name* – Name of the ACL. (Maximum length: 16 characters)
- **in** – Indicates that this list applies to ingress packets.
- **out** – Indicates that this list applies to egress packets.

Default Setting

None

Command Mode

Interface Configuration (Ethernet)

Command Usage

- A port can only be bound to one ACL.
- If a port is already bound to an ACL and you bind it to a different ACL, the switch will replace the old binding with the new one.
- You must configure a mask for an ACL rule before you can bind it to a port.

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console(config)#int eth 1/2
Console(config-if)#ip access-group standard david in
Console(config-if)#
```

Related Commands

show ip access-list (3-121)

show ip access-group

This command shows the ports assigned to IP ACLs.

Command Mode

Privileged Exec

Example

```
Console#show ip access-group
Interface ethernet 1/2
 IP standard access-list david
Console#
```

Related Commands

ip access-group (3-127)

map access-list ip

This command sets the output queue for packets matching an ACL rule. The specified CoS value is only used to map the matching packet to an output queue; it is not written to the packet itself. Use the **no** form to remove the CoS mapping.

Syntax

[**no**] **map access-list ip** *acl_name* **cos** *cos-value*

- *acl_name* – Name of the ACL. (Maximum length: 16 characters)
- *cos-value* – CoS value. (Range: 0-7)

Downloaded from www.Manualslib.com manuals search engine

Default Setting

None

Command Mode

Interface Configuration (Ethernet)

Command Usage

Command Usage

- You must configure an ACL mask before you can map CoS values to the rule.
- A packet matching a rule within the specified ACL is mapped to one of the output queues as shown in the following table. For information on mapping the CoS values to output queues, see **queue cos-map** on page 3-81.

Priority	0	1	2	3	4	5	6	7
Queue	1	2	0	3	4	5	6	7

Example

```
Console(config)#interface ethernet 1/2
Console(config-if)#map access-list ip bill cos 0
Console(config-if)#
```

Related Commands

queue cos-map (3-81)
show map access-list ip (3-129)

show map access-list ip

This command shows the CoS value mapped to an IP ACL for the current interface. (The CoS value determines the output queue for packets matching an ACL rule.)

Syntax

show map access-list ip [*interface*]

interface

Downloaded from www.Manualslib.com manuals search engine

- **ethernet** *unit/port*
  - *unit* - This is device 1.
  - *port* - Port number.

Command Mode

Privileged Exec

Example

```
Console#show map access-list ip
Access-list to COS of Eth 1/4
 Access-list ALS1 cos 0
Console#
```

Related Commands

map access-list ip (3-128)

match access-list ip

This command changes the IEEE 802.1p priority, IP Precedence, or DSCP Priority of a frame matching the defined ACL rule. (This feature is commonly referred to as ACL packet marking.) Use the **no** form to remove the ACL marker.

Syntax

match access-list ip *acl_name*
[**set priority** *priority*] {**set tos** *tos_value* | **set dscp** *dscp_value*}
no match access-list ip *acl_name*

- *acl_name* – Name of the ACL. (Maximum length: 16 characters)
- *priority* – Class of Service value in the IEEE 802.1p priority tag. (Range: 0-7; 7 is the highest priority)
- *tos_value* – IP Precedence value. (Range: 0-7)
- *dscp_value* – Differentiated Services Code Point value. (Range: 0-63)

Default Setting

None

Downloaded from www.Manualslib.com manuals search engine

Command Mode

Interface Configuration (Ethernet)

Command Usage

- You must configure an ACL mask before you can change frame priorities based on an ACL rule.
- Traffic priorities may be included in the IEEE 802.1p priority tag. This tag is also incorporated as part of the overall IEEE 802.1Q VLAN tag. To specify this priority, use the **set priority** keywords.
- The IP frame header also includes priority bits in the Type of Service (ToS) octet. The Type of Service octet may contain three bits for IP Precedence or six bits for Differentiated Services Code Point (DSCP) service. To specify the IP precedence priority, use the **set tos** keywords. To specify the DSCP priority, use the **set dscp** keywords. Note that the IP frame header can include either the IP Precedence or DSCP priority type.
- The precedence for priority mapping by this switch is IP Precedence or DSCP Priority, and then 802.1p priority.

Example

```
Console(config)#interface ethernet 1/12
Console(config-if)#match access-list ip bill set dscp 0
Console(config-if)#
```

Related Commands

show marking (3-131)

show marking

This command displays the current configuration for packet marking.

Command Mode

Privileged Exec

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console#show marking
Interface ethernet 1/12
 match access-list IP bill set DSCP 0
 match access-list MAC a set priority 0
Console#
```

Related Commands

match access-list ip (3-130)

Downloaded from www.Manualslib.com manuals search engine

MAC ACLs

Command	Function	Mode	Page
access-list mac	Creates a MAC ACL and enters configuration mode	GC	3-133
permit, deny	Filters packets matching a specified source and destination address, packet format, and Ethernet type	MAC-ACL	3-134
show mac access-list	Displays the rules for configured MAC ACLs	PE	3-136
access-list mac mask-precedence	Changes to the mode for configuring access control masks	GC	3-137
mask	Sets a precedence mask for the ACL rules	MAC-Mask	3-138
show access-list mac mask-precedence	Shows the ingress or egress rule masks for MAC ACLs	PE	3-141
mac access-group	Adds a port to a MAC ACL	IC	3-142
show mac access-group	Shows port assignments for MAC ACLs	PE	3-143
map access-list mac	Sets the CoS value and corresponding output queue for packets matching an ACL rule	IC	3-143
show map access-list mac	Shows CoS value mapped to an access list for an interface	PE	3-144
match access-list mac	Changes the 802.1p priority the priority of a frame frame matching the defined rule (i.e., also called packet marking)	IC	3-145
show marking	Displays the current configuration for packet marking	PE	3-131

access-list mac

This command adds a MAC access list and enters MAC ACL configuration mode. Use the **no** form to remove the specified ACL.

Syntax

[**no**] **access-list mac** *acl_name*

Downloaded from www.Manualslib.com manuals search engine

acl_name – Name of the ACL. (Maximum length: 16 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- An egress ACL must contain all deny rules.
- When you create a new ACL or enter configuration mode for an existing ACL, use the **permit** or **deny** command to add new rules to the bottom of the list. To create an ACL, you must add at least one rule to the list.
- To remove a rule, use the **no permit** or **no deny** command followed by the exact text of a previously configured rule.
- An ACL can contain up to 32 rules.

Example

```
Console(config)#access-list mac jerry
Console(config-mac-acl)#
```

Related Commands

permit, deny 3-134
mac access-group (3-142)
show mac access-list (3-136)

permit, **deny** (MAC ACL)

This command adds a rule to a MAC ACL. The rule filters packets matching a specified MAC source or destination address (i.e., physical layer address), or Ethernet protocol type. Use the **no** form to remove a rule.

Syntax

[**no**] {**permit** | **deny**}
{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}

Downloaded from www.Manualslib.com manuals search engine

[**vid** *vid vid-bitmask*] [**ethertype** *protocol* [*protocol-bitmask*]]

Note:- The default is for Ethernet II packets.

[**no**] {**permit** | **deny**} **tagged-eth2**
{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}
[**vid** *vid vid-bitmask*] [**ethertype** *protocol* [*protocol-bitmask*]]

[**no**] {**permit** | **deny**} **untagged-eth2**
{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}
[**ethertype** *protocol* [*protocol-bitmask*]]

[**no**] {**permit** | **deny**} **tagged-802.3**
{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}
[**vid** *vid vid-bitmask*]

[**no**] {**permit** | **deny**} **untagged-802.3**
{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}

- **tagged-eth2** – Tagged Ethernet II packets.
- **untagged-eth2** – Untagged Ethernet II packets.
- **tagged-802.3** – Tagged Ethernet 802.3 packets.
- **untagged-802.3** – Untagged Ethernet 802.3 packets.
- **any** – Any MAC source or destination address.
- **host** – A specific MAC address.
- *source* – Source MAC address.
- *destination* – Destination MAC address range with bitmask.
- *address-bitmask** – Bitmask for MAC address (in hexidecimal format).
- vid – VLAN ID. (Range: 1-4095)
- *vid-bitmask** – VLAN bitmask. (Range: 1-4095)
- *protocol* – A specific Ethernet protocol number. (Range: 600-fff hex.)
- *protocol-bitmask** – Protocol bitmask. (Range: 600-fff hex.)

* For all bitmasks, "1" means care and "0" means ignore.

Downloaded from www.Manualslib.com manuals search engine

Default Setting

None

Command Mode

MAC ACL

Command Usage

- New rules are added to the end of the list.
- The **ethertype** option can only be used to filter Ethernet II formatted packets.
- A detailed listing of Ethernet protocol types can be found in RFC 1060. A few of the more common types include the following:
  - 0800 - IP
  - 0806 - ARP
  - 8137 - IPX

Example

This rule permits packets from any source MAC address to the destination address 00-e0-29-94-34-de where the Ethernet type is 0800.

```
Console(config-mac-acl)#permit any host 00-e0-29-94-34-de ethertype 0800
Console(config-mac-acl)#
```

Related Commands

access-list mac (3-133)

show mac access-list

This command displays the rules for configured MAC ACLs.

Syntax

show mac access-list [*acl_name*]

acl_name – Name of the ACL. (Maximum length: 16 characters)

Command Mode

Privileged Exec

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console#show mac access-list
MAC access-list jerry:
  permit any 00-e0-29-94-34-de ethertype 0800
Console#
```

Related Commands

permit, deny 3-134
mac access-group (3-142)

access-list mac mask-precedence

This command changes to MAC Mask mode used to configure access control masks. Use the **no** form to delete the mask table.

Syntax

[**no**] **access-list ip mask-precedence** {**in** | **out**}

- **in** – Ingress mask for ingress ACLs.
- **out** – Egress mask for egress ACLs.

Default Setting

Default system mask: Filter inbound packets according to specified MAC ACLs.

Command Mode

Global Configuration

Command Usage

- You must configure a mask for an ACL rule before you can bind it to a port or set the queue or frame priorities associated with the rule.
- A mask can only be used by all ingress ACLs or all egress ACLs.
- The precedence of the ACL rules applied to a packet is not determined by order of the rules, but instead by the order of the masks; i.e., the first mask that matches a rule will determine the rule that is applied to a packet.

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console(config)#access-list mac mask-precedence in
Console(config-mac-mask-acl)#
```

Related Commands

mask (MAC ACL) (3-138)
mac access-group (3-142)

mask (MAC ACL)

This command defines a mask for MAC ACLs. This mask defines the fields to check in the packet header. Use the **no** form to remove a mask.

Syntax

[**no**] **mask** [**pktformat**]
{**any** | **host** | *source-bitmask*} {**any** | **host** | *destination-bitmask*}
[**vid** [*vid-bitmask*]] [**ethertype** [*ethertype-bitmask*]]

- **pktformat** – Check the packet format field. (If this keyword must be used in the mask, the packet format must be specified in ACL rule to match.)
- **any** – Any address will be matched.
- **host** – The address must be for a single node.
- *source-bitmask* – Source address of rule must match this bitmask.
- *destination-bitmask* – Destination address of rule must match this bitmask.
- **vid** – Check the VLAN ID field.
- *vid-bitmask* – VLAN ID of rule must match this bitmask.
- **ethertype** – Check the Ethernet type field.
- *ethertype-bitmask* – Ethernet type of rule must match this bitmask.

Default Setting

None

Command Mode

MAC Mask

Downloaded from www.Manualslib.com manuals search engine

Command Usage

- Up to seven masks can be assigned to an ingress or egress ACL.
- Packets crossing a port are checked against all the rules in the ACL until a match is found. The order in which these packets are checked is determined by the mask, and not the order in which the ACL rules were entered.
- First create the required ACLs and inbound or outbound masks before mapping an ACL to an interface.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to create an Ingress MAC ACL and bind it to a port. You can then see that the order of the rules have been changed by the mask.

```
Console(config)#access-list mac M4
Console(config-mac-acl)#permit any any
Console(config-mac-acl)#deny tagged-eth2 00-11-11-11-11-11
ff-ff-ff-ff-ff-ff any vid 3
Console(config-mac-acl)#end
Console#show access-list
MAC access-list M4:
  permit any any
  deny tagged-eth2 host 00-11-11-11-11-11 any vid 3
Console(config)#access-list mac mask-precedence in
Console(config-mac-mask-acl)#mask pktformat ff-ff-ff-ff-ff-ff any vid
Console(config-mac-mask-acl)#exit
Console(config)#interface ethernet 1/12
Console(config-if)#mac access-group M4 in
Console(config-if)#end
Console#show access-list
MAC access-list M4:
  deny tagged-eth2 host 00-11-11-11-11-11 any vid 3
  permit any any
MAC ingress mask ACL:
  mask pktformat host any vid
Console#
```


Downloaded from www.Manualslib.com manuals search engine

This example creates an Egress MAC ACL.

```
Console(config)#access-list mac M5
Console(config-mac-acl)#deny tagged-802.3 host 00-11-11-11-11-11 any
Console(config-mac-acl)#deny tagged-eth2 00-11-11-11-11-11
ff-ff-ff-ff-ff-ff any vid 3 ethertype 0806
Console(config-mac-acl)#end
Console#show access-list
MAC access-list M5:
  deny tagged-802.3 host 00-11-11-11-11-11 any
  deny tagged-eth2 host 00-11-11-11-11-11 any vid 3 ethertype 0806
Console(config)#access-list mac mask-precedence out
Console(config-mac-mask-acl)#mask pktformat ff-ff-ff-ff-ff-ff any vid
Console(config-mac-mask-acl)#exit
Console(config)#interface ethernet 1/5
Console(config-if)#mac access-group M5 out
Console(config-if)#end
Console#show access-list
MAC access-list M5:
  deny tagged-eth2 host 00-11-11-11-11-11 any vid 3 ethertype 0806
  deny tagged-802.3 host 00-11-11-11-11-11 any
MAC ingress mask ACL:
  mask pktformat host any vid ethertype
Console#
```

show access-list mac mask-precedence

This command shows the ingress or egress rule masks for MAC ACLs.

Syntax

show access-list mac mask-precedence [**in** | **out**]

- **in** – Ingress mask precedence for ingress ACLs.
- **out** – Egress mask precedence for egress ACLs.

Command Mode

Privileged Exec

Example

```
Console#show access-list mac mask-precedence
MAC egress mask ACL:
  mask pktformat host any vid ethertype
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Related Commands

mask (MAC ACL) (3-138)

mac access-group

This command binds a port to a MAC ACL. Use the **no** form to remove the port.

Syntax

mac access-group *acl_name* {**in** | **out**}

- *acl_name* – Name of the ACL. (Maximum length: 16 characters)
- **in** – Indicates that this list applies to ingress packets.
- **out** – Indicates that this list applies to egress packets.

Default Setting

None

Command Mode

Interface Configuration (Ethernet)

Command Usage

- A port can only be bound to one ACL.
- If a port is already bound to an ACL and you bind it to a different ACL, the switch will replace the old binding with the new one.
- You must configure a mask for an ACL rule before you can bind it to a port.

Example

```
Console(config)#interface ethernet 1/2
Console(config-if)#mac access-group jerry in
Console(config-if)#
```

Related Commands

show mac access-list (3-136)

Downloaded from www.Manualslib.com manuals search engine

show mac access-group

This command shows the ports assigned to MAC ACLs.

Command Mode

Privileged Exec

Example

```
Console#show mac access-group
Interface ethernet 1/5
 MAC access-list M5 out
Console#
```

Related Commands

mac access-group (3-142)

map access-list mac

This command sets the output queue for packets matching an ACL rule. The specified CoS value is only used to map the matching packet to an output queue; it is not written to the packet itself. Use the **no** form to remove the CoS mapping.

Syntax

[**no**] **map access-list mac** *acl_name* **cos** *cos-value*

- *acl_name* – Name of the ACL. (Maximum length: 16 characters)
- *cos-value* – CoS value. (Range: 0-7)

Default Setting

None

Command Mode

Interface Configuration (Ethernet)

Command Usage

- You must configure an ACL mask before you can map CoS values to the rule.
- A packet matching a rule within the specified ACL is mapped to one of

Downloaded from www.Manualslib.com manuals search engine

the output queues as shown below.

Priority	0	1	2	3	4	5	6	7
Queue	1	2	0	3	4	5	6	7

Example

```
Console(config)#int eth 1/5
Console(config-if)#map access-list mac M5 cos 0
Console(config-if)#
```

Related Commands

queue cos-map (3-81)
show map access-list mac (3-144)

show map access-list mac

This command shows the CoS value mapped to a MAC ACL for the current interface. (The CoS value determines the output queue for packets matching an ACL rule.)

Syntax

show map access-list mac [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - This is device 1.
  - *port* - Port number.

Command Mode

Privileged Exec

Example

```
Console#show map access-list mac
Access-list to COS of Eth 1/5
 Access-list M5 cos 0
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Related Commands

map access-list mac (3-143)

match access-list mac

This command changes the IEEE 802.1p priority of a Layer 2 frame matching the defined ACL rule. (This feature is commonly referred to as ACL packet marking.) Use the **no** form to remove the ACL marker.

Syntax

match access-list mac *acl_name* **set priority** *priority*
no match access-list mac *acl_name*

- *acl_name* – Name of the ACL. (Maximum length: 16 characters)
- *priority* – Class of Service value in the IEEE 802.1p priority tag. (Range: 0-7; 7 is the highest priority)

Default Setting

None

Command Mode

Interface Configuration (Ethernet)

Command Usage

You must configure an ACL mask before you can change frame priorities based on an ACL rule.

Example

```
Console(config)#interface ethernet 1/12
Console(config-if)#match access-list mac a set priority 0
Console(config-if)#
```

Related Commands

show marking (3-131)

Downloaded from www.Manualslib.com manuals search engine

ACL Information

Command	Function	Mode	Page
show access-list	Show all ACLs and associated rules	PE	3-146
show access-group	Shows the ACLs assigned to each port	PE	3-146

show access-list

This command shows all ACLs and associated rules, as well as all the user-defined masks.

Command Mode

Privileged Exec

Command Usage

Once the ACL is bound to an interface (i.e., the ACL is active), the order in which the rules are displayed is determined by the associated mask.

Example

```
Console#show access-list
IP standard access-list david:
  permit host 10.1.1.21
  permit 168.92.0.0 0.0.15.255
IP extended access-list bob:
  permit 10.7.1.1 0.0.0.255 any
  permit 192.168.1.0 0.0.0.255 any dport 80
  permit 192.168.1.0 0.0.0.255 any protocol tcp control-code 2 2
MAC access-list jerry:
  permit any 00-30-29-94-34-de ethertype 800
IP extended access-list A6:
  deny tcp any any control-flag 2 2
  permit any any
IP ingress mask ACL:
  mask protocol any any control-flag 2
Console#
```

show access-group

This command shows the port assignments of ACLs.

Downloaded from www.Manualslib.com manuals search engine

Command Mode

Privileged Executive

Example

```
Console#show access-group
Interface ethernet 1/2
 IP standard access-list david
 MAC access-list jerry
Console#
```

SNMP Commands

Controls access to this switch from management stations using the Simple Network Management Protocol (SNMP), as well as the error types sent to trap managers.

Command	Function	Mode	Page
snmp-server community	Sets up the community access string to permit access to SNMP commands	GC	3-147
snmp-server contact	Sets the system contact string	GC	3-148
snmp-server location	Sets the system location string	GC	3-149
snmp-server host	Specifies the recipient of an SNMP notification operation	GC	3-150
snmp-server enable traps	Enables the device to send SNMP traps (i.e., SNMP notifications)	GC	3-151
snmp ip filter	Sets IP addresses of clients allowed management access to the switch via SNMP	GC	3-152
show snmp	Displays the status of SNMP communications	NE, PE	3-154

snmp-server community

This command defines the community access string for the Simple Network Management Protocol. Use the **no** form to remove the specified community string.

Downloaded from www.Manualslib.com manuals search engine

Syntax

snmp-server community *string* [**ro**|**rw**]
no snmp-server community *string*

- *string* - Community string that acts like a password and permits access to the SNMP protocol. (Maximum length: 32 characters, case sensitive; Maximum number of strings: 5)
- **ro** - Specifies read-only access. Authorized management stations are only able to retrieve MIB objects.
- **rw** - Specifies read/write access. Authorized management stations are able to both retrieve and modify MIB objects.

Default Setting

- public - Read-only access. Authorized management stations are only able to retrieve MIB objects.
- private - Read/write access. Authorized management stations are able to both retrieve and modify MIB objects.

Command Mode

Global Configuration

Command Usage

The first **snmp-server community** command you enter enables SNMP (SNMPv1). The **no snmp-server community** command disables SNMP.

Example

```
Console(config)#snmp-server community alpha rw
Console(config)#
```

snmp-server contact

This command sets the system contact string. Use the **no** form to remove the system contact information.

Downloaded from www.Manualslib.com manuals search engine

Syntax

snmp-server contact *string*
no snmp-server contact

string - String that describes the system contact information. (Maximum length: 255 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#snmp-server contact Paul
Console(config)#
```

Related Commands

snmp-server location (3-149)

snmp-server location

This command sets the system location string. Use the **no** form to remove the location string.

Syntax

snmp-server location *text*
no snmp-server location

text - String that describes the system location. (Maximum length: 255 characters)

Default Setting

None

Command Mode

Global Configuration

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console(config)#snmp-server location WC-19
Console(config)#
```

Related Commands

snmp-server contact (3-148)

snmp-server host

This command specifies the recipient of a Simple Network Management Protocol notification operation. Use the **no** form to remove the specified host.

Syntax

snmp-server host *host-addr community-string* [**version** {**1** | **2c**}]
no snmp-server host *host-addr*

- *host-addr* - Internet address of the host (the targeted recipient). (Maximum host addresses: 5 trap destination IP address entries)
- *community-string* - Password-like community string sent with the notification operation. Although you can set this string using the **snmp-server host** command by itself, we recommend that you define this string using the **snmp-server community** command prior to using the **snmp-server host** command. (Maximum length: 32 characters)
- **version** - Specifies whether to send notifications as SNMP v1 or v2c traps.

Default Setting

Host Address: None
SNMP Version: 1

Command Mode

Global Configuration

Command Usage

- If you do not enter an **snmp-server host** command, no notifications

Downloaded from www.Manualslib.com manuals search engine

are sent. In order to configure the switch to send SNMP notifications, you must enter at least one **snmp-server host** command. In order to enable multiple hosts, you must issue a separate **snmp-server host** command for each host.

- The **snmp-server host** command is used in conjunction with the **snmp-server enable traps** command. Use the **snmp-server enable traps** command to specify which SNMP notifications are sent globally. For a host to receive notifications, at least one **snmp-server enable traps** command and the **snmp-server host** command for that host must be enabled.
- Some notification types cannot be controlled with the **snmp-server enable traps** command. For example, some notification types are always enabled.
- The switch can send SNMP version 1 or version 2c notifications to a host IP address, depending on the SNMP version that the management station supports. If the snmp-server host command does not specify the SNMP version, the default is to send SNMP version 1 notifications.

Example

```
Console(config)#snmp-server host 10.1.19.23 batman
Console(config)#
```

Related Commands

snmp-server enable traps (3-151)

snmp-server enable traps

This command enables this device to send Simple Network Management Protocol traps (SNMP notifications). Use the **no** form to disable SNMP notifications.

Syntax

[**no**] **snmp-server enable traps** [**authentication** | **link-up-down**]

- **authentication** - Keyword to issue authentication failure traps.
- **link-up-down** - Keyword to issue link-up or link-down traps.

The link-up-down trap can only be enabled/disabled via the CLI.

Downloaded from www.Manualslib.com manuals search engine

Default Setting

Issue authentication and link-up-down traps.

Command Mode

Global Configuration

Command Usage

- If you do not enter an **snmp-server enable traps** command, no notifications controlled by this command are sent. In order to configure this device to send SNMP notifications, you must enter at least one **snmp-server enable traps** command. If you enter the command with no keywords, both authentication and link-up-down notifications are enabled. If you enter the command with a keyword, only the notification type related to that keyword is enabled.
- The **snmp-server enable traps** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. In order to send notifications, you must configure at least one **snmp-server host** command.

Example

```
Console(config)#snmp-server enable traps link-up-down
Console(config)#
```

Related Commands

snmp-server host (3-150)

snmp ip filter

This command sets the IP addresses of clients that are allowed management access to the switch via SNMP. Use the **no** form the remove an IP address.

Syntax

[**no**] **snmp ip filter** *ip_address subnet_mask*

- *ip_address* - An IP address indicating a client or group of clients that

Downloaded from www.Manualslib.com manuals search engine

are allowed SNMP access to the switch.

- *subnet_mask* - An address bitmask of decimal numbers that represent the address bits to match.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- You can create a list of up to 16 IP addresses or IP address groups that are allowed access to the switch via SNMP management software.
- Address bitmasks are similar to a subnet mask, containing four decimal integers from 0 to 255, each separated by a period. The binary mask uses "1" bits to indicate "match" and "0" bits to indicate "ignore."
- If the IP is the address of a single management station, the bitmask should be set to 255.255.255.255. Otherwise, an IP address group is specified by the bitmask.
- The default setting is null, which allows all IP groups SNMP access to the switch. If one IP address is configured, IP filtering is enabled and only addresses in the specified IP group will have SNMP access.
- IP filtering does not affect management access to the switch using the web interface or Telnet.

Example

The following example enables SNMP IP filtering on the switch and allows SNMP management access to client IP 10.1.2.3, and client IP group 10.1.3.0 to 10.1.3.255.

```
Console(config)#snmp ip filter 10.1.2.3 255.255.255.255
Console(config)#snmp ip filter 10.1.3.0 255.255.255.0
Console(config)#
```

Related Commands

show snmp (3-154)

Downloaded from www.Manualslib.com manuals search engine

show snmp

This command checks the status of SNMP communications.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

This command provides information on the community access strings, counter information for SNMP input and output protocol data units, and whether or not SNMP logging has been enabled with the **snmp-server enable traps** command.

Example

```
Console#show snmp

SNMP traps:
 Authentication: enable
   Link-up-down: enable

SNMP communities:
   1. private, and the privilege is read-write
   2. public, and the privilege is read-only

0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Set-request PDUs
0 SNMP packets output
    0 Too big errors
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
    0 Trap PDUs

SNMP logging: disabled
SNMP ip filter group:
Console#
```


Downloaded from www.Manualslib.com manuals search engine

DHCP Commands

These commands are used to configure Dynamic Host Configuration Protocol (DHCP) client, relay, and server functions. You can configure any VLAN interface to be automatically assigned an IP address via DHCP. This switch can be configured to relay DHCP client configuration requests to a DHCP server on another network, or you can configure this switch to provide DHCP service directly to any client.

Command Group	Function	Page
DHCP Client	Allows interfaces to dynamically acquire IP address information	3-155
DHCP Relay	Relays DHCP requests from local hosts to a remote DHCP server	3-157
DHCP Server	Configures DHCP service using address pools or static bindings	3-160

DHCP Client

Command	Function	Mode	Page
ip dhcp client-identifier	Specifies the DHCP client identifier for this switch	IC	3-155
ip dhcp restart client	Submits a BOOTP or DHCP client request	PE	3-156

ip dhcp client-identifier

This command specifies the DCHP client identifier for the current interface. Use the **no** form to remove this identifier.

Syntax

ip dhcp client-identifier {**text** *text* | **hex** *hex*}
no ip dhcp client-identifier

- *text* - A text string. (Range: 1-15 characters)

Downloaded from www.Manualslib.com manuals search engine

- *hex* - The hexadecimal value.

Default Setting

None

Command Mode

Interface Configuration (VLAN)

Command Usage

This command is used to include a client identifier in all communications with the DHCP server. The identifier type depends on the requirements of your DHCP server.

Example

```
Console(config)#interface vlan 2
Console(config-if)#ip dhcp client-identifier hex 00-00-e8-66-65-72
Console(config-if)#
```

Related Commands

ip dhcp restart client (3-156)

ip dhcp restart client

This command submits a BOOTP or DHCP client request.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- This command issues a BOOTP or DHCP client request for any IP interface that has been set to BOOTP or DHCP mode via the **ip address** command.
- DHCP requires the server to reassign the client's last address if available.

Downloaded from www.Manualslib.com manuals search engine

- If the BOOTP or DHCP server has been moved to a different domain, the network portion of the address provided to the client will be based on this new domain.

Example

In the following example, the device is reassigned the same address.

```
Console(config)#interface vlan 1
Console(config-if)#ip address dhcp
Console(config-if)#exit
Console#ip dhcp restart client
Console#show ip interface
 IP address and netmask: 192.168.1.54 255.255.255.0 on VLAN 1,
 and address mode: Dhcp.
Console#
```

Related Commands

ip address (3-116)

DHCP Relay

Command	Function	Mode	Page
ip dhcp restart relay	Enables DHCP relay agent	IC	3-157
ip dhcp relay server	Specifies DHCP server addresses for relay	IC	3-158

ip dhcp restart relay

Use this command to enable DHCP relay for the specified VLAN. Use the **no** form to disable it.

Syntax

ip dhcp relay
no ip dhcp relay

Default Setting

Disabled

Downloaded from www.Manualslib.com manuals search engine

Command Mode

Interface Configuration (VLAN)

Command Usage

This command is used to configure DHCP relay functions for host devices attached to the switch. If DHCP relay service is enabled, and this switch sees a DHCP request broadcast, it inserts its own IP address into the request so the DHCP server will know the subnet where the client is located. Then, the switch forwards the packet to the DHCP server on another network. When the server receives the DHCP request, it allocates a free IP address for the DHCP client from its defined scope for the DHCP client's subnet, and sends a DHCP response back to the DHCP relay agent (i.e., this switch). This switch then broadcasts the DHCP response received from the server to the client.

Example

In the following example, the device is reassigned the same address.

```
Console(config)#interface vlan 1
Console(config-if)#ip dhcp relay
Console(config-if)#end
Console#show ip interface

Vlan 1 is up, addressing mode is Dhcp
  Interface address is 10.1.0.254, mask is 255.255.255.0, Primary
  MTU is 1500 bytes
  Proxy ARP is disabled
  Split horizon is enabled
Console#
```

Related Commands

ip dhcp relay server (3-158)

ip dhcp relay server

Use this command to specify the addresses of DHCP servers to be used by the switch's DHCP relay agent. Use the **no** form to clear all addresses.

Downloaded from www.Manualslib.com manuals search engine

Syntax

ip dhcp relay server *address1* [*address2* [*address3* ...]]
no ip dhcp relay server

address - IP address of DHCP server. (Range: 1-3 addresses)

Default Setting

None

Command Mode

Interface Configuration (VLAN)

Usage Guidelines

- You must specify the IP address for at least one DHCP server. Otherwise, the switch's DHCP relay agent will not forward client requests to a DHCP server.
- To start DHCP relay service, enter the **ip dhcp restart relay** command.

Example

```
Console(config)#interface vlan 1
Console(config-if)#ip dhcp relay server 10.1.0.99
Console(config-if)#
```

Related Commands

ip dhcp restart relay (3-157)

Downloaded from www.Manualslib.com manuals search engine

DHCP Server

Command	Function	Mode	Page
service dhcp	Enables the DHCP server feature on this switch	GC	3-161
ip dhcp excluded-address	Specifies IP addresses that a DHCP server should not assign to DHCP clients	GC	3-161
ip dhcp pool	Configures a DHCP address pool on a DHCP Server	GC	3-162
network	Configures the subnet number and mask for a DHCP address pool	DC	3-163
default-router	Specifies the default router list for a DHCP client	DC	3-164
domain-name	Specifies the domain name for a DHCP client	DC	3-165
dns-server	Specifies the Domain Name Server (DNS) servers available to a DHCP client	DC	3-165
next-server	Configures the next server in the boot process of a DHCP client	DC	3-166
bootfile	Specifies a default boot image for a DHCP client	DC	3-167
netbios-name-server	Configures NetBIOS Windows Internet Naming Service (WINS) name servers available to Microsoft DHCP clients	DC	3-167
netbios-node-type	Configures NetBIOS node type for Microsoft DHCP clients	DC	3-168
lease	Sets the duration an IP address is assigned to a DHCP client	DC	3-170
host*	Specifies the IP address and network mask to manually bind to a DHCP client	DC	3-170
client-identifier*	Specifies a client identifier for a DHCP client	DC	3-172
hardware-address*	Specifies the hardware address of a DHCP client	DC	3-173
clear ip dhcp binding	Deletes an automatic address binding from the DHCP server database	PE	3-174

Downloaded from www.Manualslib.com manuals search engine

Command	Function	Mode	Page
show ip dhcp binding	Displays address bindings on the DHCP server	PE, NE	3-175

*These commands are used for manually binding an address to a client.

service dhcp

Use this command to enable the DHCP server on this switch. Use the **no** form to disable the DHCP server.

Syntax

service dhcp
no service dhcp

Default Setting

Enabled

Command Mode

Global Configuration

Example

```
Console(config)#service dhcp
Console(config)#
```

ip dhcp excluded-address

Use this command to specify IP addresses that the DHCP server should not assign to DHCP clients. Use the **no** form to remove the excluded IP addresses.

Syntax

ip dhcp excluded-address *low-address* [*high-address*]
no ip dhcp excluded-address *low-address* [*high-address*]

- *low-address* - An excluded IP address, or the first IP address in an excluded address range.

Downloaded from www.Manualslib.com manuals search engine

- *high-address* - The last IP address in an excluded address range.

Default Setting

All IP pool addresses may be assigned.

Command Mode

Global Configuration

Example

```
Console(config)#ip dhcp excluded-address 10.1.0.19
Console(config)#
```

ip dhcp pool

Use this command to configure a DHCP address pool and enter DHCP Pool Configuration mode. Use the **no** form to remove the address pool.

Syntax

ip dhcp pool *name*
no ip dhcp pool *name*

name - A string or integer. (Range: 1-8 characters)

Default Setting

DHCP address pools are not configured.

Command Mode

Global Configuration

Usage Guidelines

- After executing this command, the switch changes to DHCP Pool Configuration mode, identified by the (config-dhcp)# prompt.
- From this mode, first configure address pools for the network interfaces (using the **network** command). You can also manually bind an address to a specific client (with the **host** command) if required. You can configure up to 8 network address pools, and up to 32 manually bound host address pools (i.e., listing one host address per pool). However, note that any address specified in a **host** command must fall

Downloaded from www.Manualslib.com manuals search engine

within the range of a configured network address pool.

Example

```
Console(config)#ip dhcp pool R&D
Console(config-dhcp)#
```

Related Commands

network (3-163)
host (3-170)

network

Use this command to configure the subnet number and mask for a DHCP address pool. Use the **no** form to remove the subnet number and mask.

Syntax

network *network-number* [*mask*]
no network

- *network-number* - The IP address of the DHCP address pool.
- *mask* - The bit combination that identifies the network (or subnet) and the host portion of the DHCP address pool.

Command Mode

DHCP Pool Configuration

Usage Guidelines

- When a client request is received, the switch first checks for a network address pool matching the gateway where the request originated (i.e., if the request was forwarded by a relay server). If there is no gateway in the client request (i.e., the request was not forwarded by a relay server), the switch searches for a network pool matching the interface through which the client request was received. It then searches for a manually configured host address that falls within the matching network pool. If no manually configured host address is found, it assigns an address from the matching network address pool. However, if no matching address pool is found the request is ignored.

Downloaded from www.Manualslib.com manuals search engine

- This command is valid for DHCP network address pools only. If the mask is not specified, the class A, B, or C natural mask is used (see page 3-276). The DHCP server assumes that all host addresses are available. You can exclude subsets of the address space by using the ip **dhcp excluded-address** command.

Example

```
Console(config-dhcp)#network 10.1.0.0 255.255.255.0
Console(config-dhcp)#
```

default-router

Use this command to specify default routers for a DHCP pool. Use the **no** form to remove the default routers.

Syntax

default-router *address1* [*address2*]
no default-router

- *address1* - Specifies the IP address of the primary router.
- *address2* - Specifies the IP address of an alternate router.

Default Setting

None

Command Mode

DHCP Pool Configuration

Usage Guidelines

The IP address of the router should be on the same subnet as the client. You can specify up to two routers. Routers are listed in order of preference (starting with *address1* as the most preferred router).

Example

```
Console(config-dhcp)#default-router 10.1.0.54 10.1.0.64
Console(config-dhcp)#
```


Downloaded from www.Manualslib.com manuals search engine

domain-name

Use this command to specify the domain name for a DHCP client. Use the **no** form to remove the domain name.

Syntax

domain-name *domain*
no domain-name

domain - Specifies the domain name of the client. (Range: 1-32 characters)

Default Setting

None

Command Mode

DHCP Pool Configuration

Example

```
Console(config-dhcp)#domain-name sample.com
Console(config-dhcp)#
```

dns-server

Use this command to specify the Domain Name System (DNS) IP servers available to a DHCP client. Use the **no** form to remove the DNS server list.

Syntax

dns-server *address1* [*address2*]
no dns-server

- *address1* - Specifies the IP address of the primary DNS server.
- *address2* - Specifies the IP address of the alternate DNS server.

Default Setting

None

Downloaded from www.Manualslib.com manuals search engine

Command Mode

DHCP Pool Configuration

Usage Guidelines

- If DNS IP servers are not configured for a DHCP client, the client cannot correlate host names to IP addresses.
- Servers are listed in order of preference (starting with *address1* as the most preferred server).

Example

```
Console(config-dhcp)#dns-server 10.1.1.253 192.168.3.19
Console(config-dhcp)#
```

next-server

Use this command to configure the next server in the boot process of a DHCP client. Use the **no** form to remove the boot server list.

Syntax

next-server *address*
no next-server *address*

address - Specifies the IP address of the next server in the boot process, which is typically a Trivial File Transfer Protocol (TFTP) server.

Default Setting

None

Command Mode

DHCP Pool Configuration

Example

```
Console(config-dhcp)#next-server 10.1.0.21
Console(config-dhcp)#
```

Related Commands

bootfile (3-167)

Downloaded from www.Manualslib.com manuals search engine

bootfile

Use this command to specify the name of the default boot image for a DHCP client. This file should placed on the Trivial File Transfer Protocol (TFTP) server specified with the **next-server** command. Use the **no** form to delete the boot image name.

Syntax

bootfile *filename*
no bootfile

filename - Name of the file that is used as a default boot image.

Default Setting

None

Command Mode

DHCP Pool Configuration

Example

```
Console(config-dhcp)#bootfile wme.bat
Console(config-dhcp)#
```

Related Commands

next-server (3-166)

netbios-name-server

Use this command to configure NetBIOS Windows Internet Naming Service (WINS) name servers that are available to Microsoft DHCP clients. Use the **no** form to remove the NetBIOS name server list.

Syntax

netbios-name-server *address1* [*address2*]
no netbios-name-server

- *address1* - Specifies IP address of primary NetBIOS WINS name server.

Downloaded from www.Manualslib.com manuals search engine

- *address2* - Specifies IP address of alternate NetBIOS WINS name server.

Default Setting

None

Command Mode

DHCP Pool Configuration

Usage Guidelines

Servers are listed in order of preference (starting with *address1* as the most preferred server).

Example

```
Console(config-dhcp)#netbios-name-server 10.1.0.33 10.1.0.34
Console(config-dhcp)#
```

Related Commands

netbios-node-type (3-168)

netbios-node-type

Use this command to configure the NetBIOS node type for Microsoft DHCP clients. Use the **no** form to remove the NetBIOS node type.

Syntax

netbios-node-type *type*
no netbios-node-type

type - Specifies the NetBIOS node type:

- **broadcast**
- **hybrid** (recommended)
- **mixed**
- **peer-to-peer**

Default Setting

None

Downloaded from www.Manualslib.com manuals search engine

Command Mode

DHCP Pool Configuration

Example

```
Console(config-dhcp)#netbios-node-type hybrid
Console(config-dhcp)#
```

Related Commands

netbios-name-server (3-167)

Downloaded from www.Manualslib.com manuals search engine

lease

Use this command to configure the duration that an IP address is assigned to a DHCP client. Use the **no** form to restore the default value.

Syntax

lease {*days* [*hours*][*minutes*] | **infinite**}
no lease

- *days* - Specifies the duration of the lease in numbers of days. (Range: 0-364)
- *hours* - Specifies the number of hours in the lease. A *days* value must be supplied before you can configure *hours*. (Range: 0-23)
- *minutes* - Specifies the number of minutes in the lease. A *days* and *hours* value must be supplied before you can configure *minutes*. (Range: 0-59)
- **infinite** - Specifies that the lease time is unlimited. This option is normally used for addresses manually bound to a BOOTP client via the **host** command.

Default Setting

One day

Command Modes

DHCP Pool Configuration

Example

The following example leases an address to clients using this pool for 7 days.

```
Console(config-dhcp)#lease 7
Console(config-dhcp)#
```

host

Use this command to specify the IP address and network mask to manually bind to a DHCP client. Use the **no** form to remove the IP address for the client.

Downloaded from www.Manualslib.com manuals search engine

Syntax

host *address* [*mask*]
no host

- *address* - Specifies the IP address of a client.
- *mask* - Specifies the network mask of the client.

Default Setting

None

Command Mode

DHCP Pool Configuration

Downloaded from www.Manualslib.com manuals search engine

Usage Guidelines

- Host addresses must fall within the range specified for an existing network pool.
- When a client request is received, the switch first checks for a network address pool matching the gateway where the request originated (i.e., if the request was forwarded by a relay server). If there is no gateway in the client request (i.e., the request was not forwarded by a relay server), the switch searches for a network pool matching the interface through which the client request was received. It then searches for a manually configured host address that falls within the matching network pool.
- When searching for a manual binding, the switch compares the client identifier for DHCP clients, and then compares the hardware address for DHCP or BOOTP clients.
- If no manual binding has been specified for a host entry with the **client-identifier** or **hardware-address** commands, then the switch will assign an address from the matching network pool.
- If the mask is unspecified, DHCP examines its address pools. If no mask is found in the pool database, the Class A, B, or C natural mask is used (see page 3-276). This command is valid for manual bindings only.
- The **no host** command only clears the address from the DHCP server database. It does not cancel the IP address currently in use by the host.

Example

```
Console(config-dhcp)#host 10.1.0.21 255.255.255.0
Console(config-dhcp)#
```

Related Commands

client-identifier (3-172)
hardware-address (3-173)

client-identifier

Use this command to specify the client identifier of a DHCP client. Use the **no** form to remove the client identifier.

Downloaded from www.Manualslib.com manuals search engine

Syntax

client-identifier {**text** *text* | **hex** *hex*}
no client-identifier

- *text* - A text string. (Range: 1-15 characters)
- *hex* - The hexadecimal value.

Default Setting

None

Command Mode

DHCP Pool Configuration

Command Usage

- This command identifies a DHCP client to bind to an address specified in the **host** command. If both a client identifier and hardware address are configured for a host address, the client identifier takes precedence over the hardware address in the search procedure.
- BOOTP clients cannot transmit a client identifier. To bind an address to a BOOTP client, you must associate a hardware address with the host entry.

Example

```
Console(config-dhcp)#client-identifier text steve
Console(config-dhcp)#
```

Related Commands

host (3-170)

hardware-address

Use this command to specify the hardware address of a DHCP client. This command is valid for manual bindings only. Use the **no** form to remove the hardware address.

Downloaded from www.Manualslib.com manuals search engine

Syntax

hardware-address *hardware-address type*
no hardware-address

- *hardware-address* - Specifies the MAC address of the client device.
- *type* - Indicates the following protocol used on the client device:
  - ethernet
  - ieee802
  - fddi

Default Setting

If no type is specified, the default protocol is Ethernet.

Command Mode

DHCP Pool Configuration

Command Usage

This command identifies a DHCP or BOOTP client to bind to an address specified in the **host** command. BOOTP clients cannot transmit a client identifier. To bind an address to a BOOTP client, you must associate a hardware address with the host entry.

Example

```
Console(config-dhcp)#hardware-address 00-e0-29-94-34-28 ethernet
Console(config-dhcp)#
```

Related Commands

host (3-170)

clear ip dhcp binding

Use this command to delete an automatic address binding from the DHCP server database.

Syntax

clear ip dhcp binding {*address* | ***** }

Downloaded from www.Manualslib.com manuals search engine

- *address* - The address of the binding to clear.
- ***** - Clears all automatic bindings.

Default Setting

None

Command Mode

Privileged Exec

Usage Guidelines

- An *address* specifies the client's IP address. If an asterisk (*) is used as the address parameter, the DHCP server clears all automatic bindings.
- Use the **no host** command to delete a manual binding.
- This command is normally used after modifying the address pool, or after moving DHCP service to another device.

Example.

```
Console#clear ip dhcp binding *
Console#
```

Related Commands

show ip dhcp binding (3-175)

show ip dhcp binding

Use this command to display address bindings on the DHCP server.

Syntax

show ip dhcp binding [*address*]

address - Specifies the IP address of the DHCP client for which bindings will be displayed.

Default Setting

None

Downloaded from www.Manualslib.com manuals search engine

Command Mode

Normal Exec, Privileged Exec

Example.

```
Console#show ip dhcp binding

     IP                MAC         Lease Time     Start
--------------- ----------------- ------------ -----------
     192.1.3.21 00-00-e8-98-73-21        86400 Dec 25 08:01:57 2002
Console#
```

DNS Commands

These commands are used to configure Domain Naming System (DNS) services. You can manually configure entries in the DNS domain name to IP address mapping table, configure default domain names, or specify one or more name servers to use for domain name to address translation.

Note that domain name services will not be enabled until at least one name server is specified with the **ip name-server** command and domain lookup is enabled with the **ip domain-lookup** command.

Command	Function	Mode	Page
ip host	Creates a static host name-to-address mapping	GC	3-177
clear host	Deletes entries from the host name-to-address table	PE	3-178
ip domain-name	Defines a default domain name for incomplete host names	GC	3-178
ip domain-list	Defines a list of default domain names for incomplete host names	GC	3-179
ip name-server	Specifies the address of one or more name servers to use for host name-to-address translation	GC	3-181
ip domain-lookup	Enables DNS-based host name-to-address translation	GC	3-182

Downloaded from www.Manualslib.com manuals search engine

Command	Function	Mode	Page
show hosts	Displays the static host name-to-address mapping table	PE	3-183
show dns	Displays the configuration for DNS services	PE	3-184
show dns cache	Displays entries in the DNS cache	PE	3-184
clear dns cache	Clears all entries from the DNS cache	PE	3-185

ip host

This command creates a static entry in the DNS table that maps a host name to an IP address. Use the **no** form to remove an entry.

Syntax

[**no**] **ip host** *name address1* [*address2* … *address8*]

- *name* - Name of the host. (Range: 1-64 characters)
- *address1* - Corresponding IP address.
- *address2* … *address8* - Additional corresponding IP addresses.

Default Setting

No static entries

Command Mode

Global Configuration

Command Usage

Servers or other network devices may support one or more connections via multiple IP addresses. If more than one IP address is associated with a host name using this command, a DNS client can try each address in succession, until it establishes a connection with the target device.

Downloaded from www.Manualslib.com manuals search engine

Example

This example maps two address to a host name.

```
Console(config)#ip host rd5 192.168.1.55 10.1.0.55
Console(config)#end
Console#show hosts

Hostname
 rd5
Inet address
 10.1.0.55 192.168.1.55
Alias
Console#
```

clear host

This command deletes entries from the DNS table.

Syntax

clear host {*name* | *}

- *name* - Name of the host. (Range: 1-64 characters)
- * - Removes all entries.

Default Setting

None

Command Mode

Privileged Exec

Example

This example clears all static entries from the DNS table.

```
Console(config)#clear host *
Console(config)#
```

ip domain-name

This command defines the default domain name appended to incomplete host names (i.e., host names passed from a client that are not formatted

Downloaded from www.Manualslib.com manuals search engine

with dotted notation). Use the **no** form to remove the current domain name.

Syntax

ip domain-name *name*
no ip domain-name

name - Name of the host. Do not include the initial dot that separates the host name from the domain name.
(Range: 1-64 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#ip domain-name sample.com
Console(config)#end
Console#show dns
Domain Lookup Status:
    DNS disabled
Default Domain Name:
    .sample.com
Domain Name List:
Name Server List:
Console#
```

Related Commands

ip domain-list (3-179)
ip name-server (3-181)
ip domain-lookup (3-182)

ip domain-list

This command defines a list of domain names that can be appended to incomplete host names (i.e., host names passed from a client that are not formatted with dotted notation). Use the **no** form to remove a name from this list.

Downloaded from www.Manualslib.com manuals search engine

Syntax

[**no**] **ip domain-list** *name*

name - Name of the host. Do not include the initial dot that separates the host name from the domain name.
(Range: 1-64 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- Domain names are added to the end of the list one at a time.
- When an incomplete host name is received by the DNS server on this switch, it will work through the domain list, appending each domain name in the list to the host name, and checking with the specified name servers for a match.
- If there is no domain list, the domain name specified with the **ip domain-name** command is used. If there is a domain list, the default domain name is not used.

Example

This example adds two domain names to the current list and then displays the list.

```
Console(config)#ip domain-list sample.com.jp
Console(config)#ip domain-list sample.com.uk
Console(config)#end
Console#show dns
Domain Lookup Status:
    DNS disabled
Default Domain Name:
    .sample.com
Domain Name List:
    .sample.com.jp
    .sample.com.uk
Name Server List:
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Related Commands

ip domain-name (3-178)

ip name-server

This command specifies the address of one or more domain name servers to use for name-to-address resolution. Use the **no** form to remove a name server from this list.

Syntax

[**no**] **ip name-server** *server-address1* [*server-address2* … *server-address6*]

- *server-address1* - IP address of domain-name server.
- *server-address2* … *server-address6* - IP address of additional domain-name servers.

Default Setting

None

Command Mode

Global Configuration

Command Usage

The listed name servers are queried in the specified sequence until a response is received, or the end of the list is reached with no response.

Downloaded from www.Manualslib.com manuals search engine

Example

This example adds two domain-name servers to the list and then displays the list.

```
Console(config)#ip domain-server 192.168.1.55 10.1.0.55
Console(config)#end
Console#show dns
Domain Lookup Status:
    DNS disabled
Default Domain Name:
    .sample.com
Domain Name List:
    .sample.com.jp
    .sample.com.uk
Name Server List:
    192.168.1.55
    10.1.0.55
Console#
```

Related Commands

ip domain-name (3-178)
ip domain-lookup (3-182)

ip domain-lookup

This command enables DNS host name-to-address translation. Use the **no** form to disable DNS.

Syntax

[**no**] **ip domain-lookup**

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- At least one name server must be specified before you can enable DNS.
- If all name servers are deleted, DNS will automatically be disabled.

Downloaded from www.Manualslib.com manuals search engine

Example

This example enables DNS and then displays the configuration.

```
Console(config)#ip domain-lookup
Console(config)#end
Console#show dns
Domain Lookup Status:
    DNS enabled
Default Domain Name:
    .sample.com
Domain Name List:
    .sample.com.jp
    .sample.com.uk
Name Server List:
    192.168.1.55
    10.1.0.55
Console#
```

Related Commands

ip domain-name (3-178)
ip name-server (3-181)

show hosts

This command displays the static host name-to-address mapping table.

Command Mode

Privileged Exec

Example

Note that a host name will be displayed as an alias if it is mapped to the same address(es) as a previously configured entry.

```
Console#show hosts

Hostname
 rd5
Inet address
 10.1.0.55 192.168.1.55
Alias
 1.rd6
Console#
```


Downloaded from www.Manualslib.com manuals search engine

show dns

This command displays the configuration of the DNS server.

Command Mode

Privileged Exec

Example

```
Console#show dns
Domain Lookup Status:
    DNS enabled
Default Domain Name:
    sample.com
Domain Name List:
    sample.com.jp
    sample.com.uk
Name Server List:
    192.168.1.55
    10.1.0.55
Console#
```

show dns cache

This command displays entries in the DNS cache.

Command Mode

Privileged Exec

Example

```
Console#show dns cache
NO      FLAG    TYPE    IP              TTL     DOMAIN
0        4      CNAME   10.2.44.96      893     pttch_pc.accton.com.tw
1        4      CNAME   10.2.44.3       898     ahten.accton.com.tw
2        4      CNAME   66.218.71.84    298     www.yahoo.akadns.net
3        4      CNAME   66.218.71.83    298     www.yahoo.akadns.net
4        4      CNAME   66.218.71.81    298     www.yahoo.akadns.net
5        4      CNAME   66.218.71.80    298     www.yahoo.akadns.net
6        4      CNAME   66.218.71.89    298     www.yahoo.akadns.net
7        4      CNAME   66.218.71.86    298     www.yahoo.akadns.net
8        4      ALIAS   POINTER TO:7    298     www.yahoo.com
Console#
```

Field	Description
NO	The entry number for each resource record.

Downloaded from www.Manualslib.com manuals search engine

Field	Description
FLAG	The flag is always "4" indicating a cache entry and therefore unreliable.
TYPE	This field includes CNAME which specifies the canonical or primary name for the owner, and ALIAS which specifies multiple domain names which are mapped to the same IP address as an existing entry.
IP	The IP address associated with this record.
TTL	The time to live reported by the name server.
DOMAIN	The domain name associated with this record.

clear dns cache

This command clears all entries in the DNS cache.

Command Mode

Privileged Exec

Example

```
Console#clear dns cache
Console#show dns cache
NO      FLAG    TYPE    IP              TTL     DOMAIN
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

Interface Commands

These commands are used to display or set communication parameters for an Ethernet port, aggregated link, or VLAN.

Command	Function	Mode	Page
interface	Configures an interface type and enters interface configuration mode	GC	3-1
description	Adds a description to an interface configuration	IC	3-2
speed-duplex	Configures the speed and duplex operation of a given interface when autonegotiation is disabled	IC	3-3
negotiation	Enables autonegotiation of a given interface	IC	3-4
capabilities	Advertises the capabilities of a given interface for use in autonegotiation	IC	3-5
flowcontrol	Enables flow control on a given interface	IC	3-7
combo-forced-mode	Force port type selected for combination ports	IC	3-8
shutdown	Disables an interface	IC	3-9
switchport broadcast packet-rate	Configures the broadcast storm control threshold	IC	3-9
clear counters	Clears statistics on an interface	PE	3-10
show interfaces status	Displays status for the specified interface	NE, PE	3-11
show interfaces counters	Displays statistics for the specified interfaces	NE, PE	3-13
show interfaces switchport	Displays the administrative and operational status of an interface	NE, PE	3-14

interface

This command configures an interface type and enter interface configuration mode. Use the **no** form to remove a trunk.

Downloaded from www.Manualslib.com manuals search engine

Syntax

interface *interface*
no interface port-channel *channel-id*

interface

- **ethernet** *unit/port*
  - *unit* - This is device 1.
  - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-6)
- **vlan** *vlan-id* (Range: 1-4094)

Default Setting

None

Command Mode

Global Configuration

Example

To specify port 4, enter the following command:

```
Console(config)#interface ethernet 1/4
Console(config-if)#
```

description

This command adds a description to an interface. Use the **no** form to remove the description.

Syntax

description *string*
no description

string - Comment or a description to help you remember what is attached to this interface. (Range: 1-64 characters)

Default Setting

None

Downloaded from www.Manualslib.com manuals search engine

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

The following example adds a description to port 4.

```
Console(config)#interface ethernet 1/4
Console(config-if)#description RD-SW#3
Console(config-if)#
```

speed-duplex

This command configures the speed and duplex mode of a given interface when autonegotiation is disabled. Use the **no** form to restore the default.

Syntax

speed-duplex {**1000full** | **100full** | **100half** | **10full** | **10half**}
no speed-duplex

- **1000full** - Forces 1000 Mbps full-duplex operation
- **100full** - Forces 100 Mbps full-duplex operation
- **100half** - Forces 100 Mbps half-duplex operation
- **10full** - Forces 10 Mbps full-duplex operation
- **10half** - Forces 10 Mbps half-duplex operation

Downloaded from www.Manualslib.com manuals search engine

Default Setting

- Auto-negotiation is enabled by default.
- When auto-negotiation is disabled, the default speed-duplex setting is 100half for 100BASE-TX ports and 1000full for Gigabit Ethernet ports.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- To force operation to the speed and duplex mode specified in a **speed-duplex** command, use the **no negotiation** command to disable auto-negotiation on the selected interface.
- When using the **negotiation** command to enable auto-negotiation, the optimal settings will be determined by the **capabilities** command. To set the speed/duplex mode under auto-negotiation, the required mode must be specified in the capabilities list for an interface.

Example

The following example configures port 5 to 100 Mbps, half-duplex operation.

```
Console(config)#interface ethernet 1/5
Console(config-if)#speed-duplex 100half
Console(config-if)#no negotiation
Console(config-if)#
```

Related Commands

negotiation (3-4)
capabilities (3-5)

negotiation

This command enables autonegotiation for a given interface. Use the **no** form to disable autonegotiation.

Syntax

[**no**] **negotiation**

Downloaded from www.Manualslib.com manuals search engine

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- When auto-negotiation is enabled the switch will negotiate the best settings for a link based on the **capabilities** command. When auto-negotiation is disabled, you must manually specify the link attributes with the **speed-duplex** and **flowcontrol** commands.
- If autonegotiation is disabled, auto-MDI/MDI-X pin signal configuration will also be disabled for the RJ-45 ports.

Example

The following example configures port 11 to use autonegotiation.

```
Console(config)#interface ethernet 1/11
Console(config-if)#negotiation
Console(config-if)#
```

Related Commands

capabilities (3-5)
speed-duplex (3-3)

capabilities

This command advertises the port capabilities of a given interface during autonegotiation. Use the **no** form with parameters to remove an advertised capability, or the **no** form without parameters to restore the default values.

Syntax

[**no**] **capabilities** {**1000full** | **100full** | **100half** | **10full** | **10half** | **flowcontrol** | **symmetric**}

- **1000full** - Supports 1000 Mbps full-duplex operation
- **100full** - Supports 100 Mbps full-duplex operation
- **100half** - Supports 100 Mbps half-duplex operation

Downloaded from www.Manualslib.com manuals search engine

- **10full** - Supports 10 Mbps full-duplex operation
- **10half** - Supports 10 Mbps half-duplex operation
- **flowcontrol** - Supports flow control
- **symmetric** (Gigabit only) - When specified, the port transmits and receives pause frames; when not specified, the port will auto-negotiate to determine the sender and receiver for asymmetric pause frames. (*The current switch ASIC only supports symmetric pause frames.*)

Default Setting

- 100BASE-TX: 10half, 10full, 100half, 100full
- 1000BASE-T: 10half, 10full, 100half, 100full, 1000full
- 1000BASE-SX/LX/LH: 1000full

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

When auto-negotiation is enabled with the **negotiation** command, the switch will negotiate the best settings for a link based on the **capabilites** command. When auto-negotiation is disabled, you must manually specify the link attributes with the **speed-duplex** and **flowcontrol** commands.

Example

The following example configures Ethernet port 5 capabilities to 100half, 100full and flow control.

```
Console(config)#interface ethernet 1/5
Console(config-if)#capabilities 100half
Console(config-if)#capabilities 100full
Console(config-if)#capabilities flowcontrol
Console(config-if)#
```

Related Commands

negotiation (3-4)
speed-duplex (3-3)

Downloaded from www.Manualslib.com manuals search engine

flowcontrol (3-7)

flowcontrol

This command enables flow control. Use the **no** form to disable flow control.

Syntax

[**no**] **flowcontrol**

Default Setting

Flow control enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Flow control can eliminate frame loss by "blocking" traffic from end stations or segments connected directly to the switch when its buffers fill. When enabled, back pressure is used for half-duplex operation and IEEE 802.3x for full-duplex operation.
- To force flow control on or off (with the **flowcontrol** or **no flowcontrol** command), use the **no negotiation** command to disable auto-negotiation on the selected interface.
- When using the **negotiation** command to enable auto-negotiation, the optimal settings will be determined by the **capabilities** command. To enable flow control under auto-negotiation, "flowcontrol" must be included in the capabilities list for any port
- Avoid using flow control on a port connected to a hub unless it is actually required to solve a problem. Otherwise back pressure jamming signals may degrade overall performance for the segment attached to the hub.

Downloaded from www.Manualslib.com manuals search engine

Example

The following example enables flow control on port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#flowcontrol
Console(config-if)#no negotiation
Console(config-if)#
```

Related Commands

negotiation (3-4)
capabilities (flowcontrol, symmetric) (3-5)

combo-forced-mode

This command forces the port type selected for combination ports 8 - 12. Use the **no** form to restore the default mode.

Syntax

combo-forced-mode *mode*
no combo-forced-mode

- *mode*
  - **copper-forced** - Always uses the built-in RJ-45 port.
  - **copper-preferred-auto** - Uses the built-in RJ-45 port if both combination types are functioning and the RJ-45 port has a valid link.
  - **sfp-forced** - Always uses the SFP port (even if module not installed).
  - **sfp-preferred-auto** - Uses SFP port if both combination types are functioning and the SFP port has a valid link.

Default Setting

sfp-preferred-auto

Command Mode

Interface Configuration (Ethernet)

Downloaded from www.Manualslib.com manuals search engine

Example

This forces the switch to use the built-in RJ-45 port for the combination port 8.

```
Console(config)#interface ethernet 1/8
Console(config-if)#combo-forced-mode copper-forced
Console(config-if)#
```

shutdown

This command disables an interface. To restart a disabled interface, use the **no** form.

Syntax

[**no**] **shutdown**

Default Setting

All interfaces are enabled.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

This command allows you to disable a port due to abnormal behavior (e.g., excessive collisions), and then reenable it after the problem has been resolved. You may also want to disable a port for security reasons.

Example

The following example disables port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#shutdown
Console(config-if)#
```

switchport broadcast packet-rate

This command configures broadcast storm control. Use the **no** form to disable broadcast storm control.

Downloaded from www.Manualslib.com manuals search engine

Syntax

switchport broadcast packet-rate *rate*
no switchport broadcast

rate - Threshold level as a rate; i.e., packets per second. (Range: 500 - 262143)

Default Setting

Enabled for all ports
Packet-rate limit: 500 packets per second

Command Mode

Interface Configuration (Ethernet)

Command Usage

- When broadcast traffic exceeds the specified threshold, packets above that threshold are dropped.
- This command can enable or disable broadcast storm control for the selected interface. However, the specified threshold value applies to all ports on the switch.

Example

The following shows how to configure broadcast storm control at 600 packets per second:

```
Console(config)#interface ethernet 1/5
Console(config-if)#switchport broadcast packet-rate 600
Console(config-if)#
```

clear counters

This command clears statistics on an interface.

Syntax

clear counters *interface*

interface

- **ethernet** *unit/port*

Downloaded from www.Manualslib.com manuals search engine

- *unit* - This is device 1.
- *port* - Port number.
  - **port-channel** *channel-id* (Range: 1-6)

Default Setting

None

Command Mode

Privileged Exec

Command Usage

Statistics are only initialized for a power reset. This command sets the base value for displayed statistics to zero for the current management session. However, if you log out and back into the management interface, the statistics displayed will show the absolute value accumulated since the last power reset.

Example

The following example clears statistics on port 5.

```
Console#clear counters ethernet 1/5
Console#
```

show interfaces status

This command displays the status for an interface.

Syntax

show interfaces status [*interface*]

interface

- **ethernet** *unit/port*
- *unit* - This is device 1.
- *port* - Port number.
  - **port-channel** *channel-id* (Range: 1-6)
  - **vlan** *vlan-id* (Range: 1-4094)

Downloaded from www.Manualslib.com manuals search engine

Default Setting

Shows the status for all interfaces.

Command Mode

Normal Exec, Privileged Exec

Command Usage

If no interface is specified, information on all interfaces is displayed. For a description of the items displayed by this command, see "Displaying Connection Status" on page 3-89.

Example

```
Console#show interfaces status ethernet 1/5
Information of Eth 1/5
 Basic information:
  Port type: 1000T
  Mac address: 00-00-AB-CD-00-01
 Configuration:
  Name:
  Port admin: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full, 1000full,
  Broadcast storm: Enabled
  Broadcast storm limit: 500 packets/second
  Flow control: Disabled
  Lacp: Disabled
  Port security: Disabled
  Max MAC count: 0
  Port security action: None
  Combo forced mode: None
Current status:
  Link status: Up
  Port operation status: Up
  Operation speed-duplex: 1000full
  Flow control type: None
Console#show interfaces status vlan 1
 Information of VLAN 1
 MAC address: 00-00-AB-CD-00-00
Console#
```


Downloaded from www.Manualslib.com manuals search engine

show interfaces counters

This command displays interface statistics.

Syntax

show interfaces counters [*interface*]

interface

- **ethernet** *unit*/*port*

- *unit* - This is device 1.
- *port* - Port number.
  - **port-channel** *channel-id* (Range: 1-6)

Default Setting

Shows the counters for all interfaces.

Command Mode

Normal Exec, Privileged Exec

Command Usage

If no interface is specified, information on all interfaces is displayed. For a description of the items displayed by this command, see "Showing Port Statistics" on page 3-116.

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console#show interfaces counters ethernet 1/7
Ethernet 1/7
 Iftable stats:
  Octets input: 30658, Octets output: 196550
  Unicast input: 6, Unicast output: 5
  Discard input: 0, Discard output: 0
  Error input: 0, Error output: 0
  Unknown protos input: 0, QLen output: 0
 Extended iftable stats:
  Multi-cast input: 0, Multi-cast output: 3064
  Broadcast input: 262, Broadcast output: 1
 Ether-like stats:
  Alignment errors: 0, FCS errors: 0
  Single Collision frames: 0, Multiple collision frames: 0
  SQE Test errors: 0, Deferred transmissions: 0
  Late collisions: 0, Excessive collisions: 0
  Internal mac transmit errors: 0, Internal mac receive errors: 0
  Frame too longs: 0, Carrier sense errors: 0
  Symbol errors: 0
 RMON stats:
  Drop events: 0, Octets: 227208, Packets: 3338
  Broadcast pkts: 263, Multi-cast pkts: 3064
  Undersize pkts: 0, Oversize pkts: 0
  Fragments: 0, Jabbers: 0
  CRC align errors: 0, Collisions: 0
  Packet size <= 64 octets: 3150, Packet size 65 to 127 octets: 139
  Packet size 128 to 255 octets: 49, Packet size 256 to 511 octets: 0
  Packet size 512 to 1023 octets: 0, Packet size 1024 to 1518 octets: 0
Console#
```

show interfaces switchport

This command displays the administrative and operational status of the specified interfaces.

Syntax

show interfaces switchport [*interface*]

interface

- **ethernet** *unit/port*

- *unit* - This is device 1.
- *port* - Port number.
  - **port-channel** *channel-id* (Range: 1-6)

Downloaded from www.Manualslib.com manuals search engine

Default Setting

Shows all interfaces.

Command Mode

Normal Exec, Privileged Exec

Command Usage

If no interface is specified, information on all interfaces is displayed.

Example

This example shows the configuration setting for port 4.

```
Console#show interfaces switchport ethernet 1/4
 Broadcast threshold: Enabled, 500 packets/second
 Lacp status: Disabled
 Ingress rate limit: disable,1000M bits per second
 Egress rate limit: disable,1000M bits per second
 VLAN membership mode: Hybrid
 Ingress rule: Disabled
 Acceptable frame type: All frames
 Native VLAN: 1
 Priority for untagged traffic: 0
 Gvrp status: Disabled
 Allowed Vlan:    1(u),
 Forbidden Vlan:
Console#
```

Field	Description
Broadcast threshold	Shows if broadcast storm suppression is enabled or disabled; if enabled it also shows the threshold level (page 3-9).
Lacp status	Shows if Link Aggregation Control Protocol has been enabled or disabled (page 3-22).
Ingress/Egress rate limit	Shows if rate limiting is enabled, and the current rate limit (page 3-19).
VLAN membership mode	Indicates membership mode as Trunk or Hybrid (page 3-58).
Ingress rule	Shows if ingress filtering is enabled or disabled (page 3-60).
Acceptable frame type	Shows if acceptable VLAN frames include all types or tagged frames only (page 3-59).
Native VLAN	Indicates the default Port VLAN ID (page 3-61).

Downloaded from www.Manualslib.com manuals search engine

Field	Description
Priority for untagged traffic	Indicates the default priority for untagged frames (page 3-77).
Gvrp status	Shows if GARP VLAN Registration Protocol is enabled or disabled (page 3-73).
Allowed Vlan	Shows the VLANs this interface has joined, where "(u)" indicates untagged and "(t)" indicates tagged (page 3-62).
Forbidden Vlan	Shows the VLANs this interface can not dynamically join via GVRP (page 3-63).

Mirror Port Commands

This section describes how to mirror traffic from a source port to a target port.

Command	Function	Mode	Page
port monitor	Configures a mirror session	IC	3-16
show port monitor	Shows the configuration for a mirror port	PE	3-17

port monitor

This command configures a mirror session. Use the **no** form to clear a mirror session.

Syntax

port monitor *interface* [**rx** | **tx** | **both**]
no port monitor *interface*

- *interface* - **ethernet** *unit*/*port* (source port)
  - *unit* - Switch (unit 1).
  - *port* - Port number.
- **rx** - Mirror received packets.
- **tx** - Mirror transmitted packets.
- **both** - Mirror both received and transmitted packets.

Downloaded from www.Manualslib.com manuals search engine

Default Setting

No mirror session is defined. When enabled, the default mirroring is for both received and transmitted packets.

Command Mode

Interface Configuration (Ethernet, destination port)

Command Usage

- You can mirror traffic from any source port to a destination port for real-time analysis. You can then attach a logic analyzer or RMON probe to the destination port and study the traffic crossing the source port in a completely unobtrusive manner.
- The destination port is set by specifying an Ethernet interface.
- The mirror port and monitor port speeds should match, otherwise traffic may be dropped from the monitor port.
- You can create multiple mirror sessions, but all sessions must share the same destination port. However, you should avoid sending too much traffic to the destination port from multiple source ports.

Example

The following example configures the switch to mirror all packets from port 6 to 11:

```
Console(config)#interface ethernet 1/11
Console(config-if)#port monitor ethernet 1/6 both
Console(config-if)#
```

show port monitor

This command displays mirror information.

Syntax

show port monitor [*interface*]

interface - **ethernet** *unit*/*port* (source port)

- *unit* - Switch (unit 1).
- *port* - Port number.

Downloaded from www.Manualslib.com manuals search engine

Default Setting

Shows all sessions.

Command Mode

Privileged Exec

Command Usage

This command displays the currently configured source port, destination port, and mirror mode (i.e., RX, TX, RX/TX).

Example

The following shows mirroring configured from port 6 to port 11:

```
Console(config)#interface ethernet 1/11
Console(config-if)#port monitor ethernet 1/6
Console(config-if)#end
Console#show port monitor
Port Mirroring
-------------------------------------
 Destination port(listen port):Eth1/1
 Source port(monitored port)  :Eth1/6
 Mode                         :RX/TX
Console#
```

Rate Limit Commands

This function allows the network manager to control the maximum rate for traffic transmitted or received on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic into or out of the network. Traffic that falls within the rate limit is transmitted, while packets that exceed the acceptable amount of traffic are dropped.

Rate limiting can be applied to individual ports or trunks. When an interface is configured with this feature, the traffic rate will be monitored

Downloaded from www.Manualslib.com manuals search engine

by the hardware to verify conformity. Non-conforming traffic is dropped, conforming traffic is forwarded without any changes.

Command	Function	Mode	Page
rate-limit	Configures the maximum input or output rate for a port	IC	3-19

rate-limit

This command defines the rate limit for a specific interface. Use this command without specifying a rate to restore the default rate. Use the **no** form to restore the default status of disabled.

Syntax

rate-limit {**input** | **output**} [*rate*]
no rate-limit {**input** | **output**}

- **input** – Input rate
- **output** – Output rate
- *rate* – Maximum value in Mbps. (Range: 1 to 1000 Mbps)

Default Setting

1000 Mbps

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#rate-limit input 600
Console(config-if)#
```


Downloaded from www.Manualslib.com manuals search engine

Link Aggregation Commands

Ports can be statically grouped into an aggregate link (i.e., trunk) to increase the bandwidth of a network connection or to ensure fault recovery. Or you can use the Link Aggregation Control Protocol (LACP) to automatically negotiate a trunk link between this switch and another network device. For static trunks, the switches have to comply with the Cisco EtherChannel standard. For dynamic trunks, the switches have to comply with LACP. This switch supports up to six trunks. For example, a trunk consisting of two 1000 Mbps ports can support an aggregate bandwidth of 4 Gbps when operating at full duplex.

Command	Function	Mode	Page
Manual Configuration Commands			
interface port-channel	Configures a trunk and enters interface configuration mode for the trunk	GC	3-1
channel-group	Adds a port to a trunk	IC (Ethernet)	3-21
Dynamic Configuration Command			
lacp	Configures LACP for the current interface	IC (Ethernet)	3-22
lacp system-priority	Configures a port's LACP system priority	IC (Ethernet)	3-24
lacp admin-key	Configures a port's administration key	IC (Ethernet)	3-25
lacp admin-key	Configures an port channel's administration key	IC (Port Channel)	3-26
lacp port-priority	Configures a port's LACP port priority	IC (Ethernet)	3-27
Trunk Status Display Command			
show interfaces status port-channel	Shows trunk information	NE, PE	3-11
show lacp	Shows LACP information	PE	3-28

Guidelines for Creating Trunks

General Guidelines –

- Finish configuring port trunks before you connect the corresponding network cables between switches to avoid creating a loop.

Downloaded from www.Manualslib.com manuals search engine

- A trunk can have up to eight ports.
- The ports at both ends of a connection must be configured as trunk ports.
- All ports in a trunk must be configured in an identical manner, including communication mode (i.e., speed, duplex mode and flow control), VLAN assignments, and CoS settings.
- All the ports in a trunk have to be treated as a whole when moved from/to, added or deleted from a VLAN via the specified port-channel.
- STP, VLAN, and IGMP settings can only be made for the entire trunk via the specified port-channel.
- Dynamically Creating a Port Channel –
- Ports assigned to a common port channel must meet the following criteria:
- Ports must have the same LACP system priority.
- Ports must have the same port admin key (Ethernet Interface).
- If the port channel admin key (lacp admin key - Port Channel) is not set when a channel group is formed (i.e., it has the null value of 0), this key is set to the same value as the port admin key (lacp admin key - Ethernet Interface) used by the interfaces that joined the group.
- However, if the port channel admin key is set, then the port admin key must be set to the same value for a port to be allowed to join a channel group.
- If a link goes down, LACP port priority is used to select the backup link.

channel-group

This command adds a port to a trunk. Use the **no** form to remove a port from a trunk.

Syntax

channel-group *channel-id*
no channel-group

channel-id - Trunk index (Range: 1-6)

Downloaded from www.Manualslib.com manuals search engine

Default Setting

The current port will be added to this trunk.

Command Mode

Interface Configuration (Ethernet)

Command Usage

- When configuring static trunks, the switches must comply with the Cisco EtherChannel standard.
- Use **no channel-group** to remove a port group from a trunk.
- Use **no interfaces port-channel** to remove a trunk from the switch.

Example

The following example creates trunk 1 and then adds port 11:

```
Console(config)#interface port-channel 1
Console(config-if)#exit
Console(config)#interface ethernet 1/11
Console(config-if)#channel-group 1
Console(config-if)#
```

lacp

This command enables 802.3ad Link Aggregation Control Protocol (LACP) for the current interface. Use the **no** form to disable it.

Syntax

[**no**] **lacp**

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet)

Downloaded from www.Manualslib.com manuals search engine

Command Usage

- The ports on both ends of an LACP trunk must be configured for full duplex, either by forced mode or auto-negotiation.
- A trunk formed with another switch using LACP will automatically be assigned the next available port-channel ID.
- If the target switch has also enabled LACP on the connected ports, the trunk will be activated automatically.
- If more than four ports attached to the same target switch have LACP enabled, the additional ports will be placed in standby mode, and will only be enabled if one of the active links fails.

Example

The following shows LACP enabled on ports 10-12. Because LACP has also been enabled on the ports at the other end of the links, the **show interfaces status port-channel 1** command shows that Trunk1 has been established.

```
Console(config)#interface ethernet 1/10
Console(config-if)#lacp
Console(config-if)#exit
Console(config)#interface ethernet 1/11
Console(config-if)#lacp
Console(config-if)#exit
Console(config)#interface ethernet 1/12
Console(config-if)#lacp
Console(config-if)#exit
Console(config)#exit
Console#show interfaces status port-channel 1
Information of Trunk 1
 Basic information:
  Port type: 1000T
  Mac address: 00-00-e8-00-00-0b
 Configuration:
  Name:
  Port admin status: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full, 1000full,
  Flow control status: Disabled
  Port security: Disabled
  Max MAC count: 0
```


Downloaded from www.Manualslib.com manuals search engine

```
 Current status:
  Created by: lacp
  Link status: Up
  Operation speed-duplex: 1000full
  Flow control type: None
  Member Ports: Eth1/10, Eth1/11, Eth1/12,
Console#
```

lacp system-priority

This command configures a port's LACP system priority. Use the **no** form to restore the default setting.

Syntax

lacp {**actor** | **partner**} **system-priority** *priority*
no lacp {**actor** | **partner**} **system-priority**

- **actor** - The local side an aggregate link.
- **partner** - The remote side of an aggregate link.
- *priority* - This priority is used to determine link aggregation group (LAG) membership, and to identify this device to other switches during LAG negotiations. (Range: 0-65535)

Default Setting

32768

Command Mode

Interface Configuration (Ethernet)

Command Usage

- Port must be configured with the same system priority to join the same LAG.
- System priority is combined with the switch's MAC address to form the LAG identifier. This identifier is used to indicate a specific LAG during LACP negotiations with other systems.
- Once the remote side of a link has been established, LACP operational settings are already in use on that side. Configuring LACP settings for the partner only applys to its administrative state, not its operational

Downloaded from www.Manualslib.com manuals search engine

state, and will only take effect the next time an aggregate link is established with the partner.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor system-priority 3
Console(config-if)#
```

lacp admin-key (Ethernet Interface)

This command configures a port's LACP administration key. Use the **no** form to restore the default setting.

Syntax

lacp {**actor** | **partner**} **admin-key** *key*
[**no**] **lacp** {**actor** | **partner**} **admin-key**

- **actor** - The local side an aggregate link.
- **partner** - The remote side of an aggregate link.
- *key* - The port admin key must be set to the same value for ports that belong to the same link aggregation group (LAG). (Range: 0-65535)

Default Setting

0

Command Mode

Interface Configuration (Ethernet)

Command Usage

- Ports are only allowed to join the same LAG if (1) the LACP system priority matches, (2) the LACP port admin key matches, and (3) the LACP port channel key matches (if configured).
- If the port channel admin key (**lacp admin key** - Port Channel) is not set when a channel group is formed (i.e., it has the null value of 0), this key is set to the same value as the port admin key (**lacp admin key** - Ethernet Interface) used by the interfaces that joined the group.

Downloaded from www.Manualslib.com manuals search engine

- Once the remote side of a link has been established, LACP operational settings are already in use on that side. Configuring LACP settings for the partner only applys to its administrative state, not its operational state, and will only take effect the next time an aggregate link is established with the partner.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor admin-key 120
Console(config-if)#
```

lacp admin-key (Port Channel)

This command configures a port channel's LACP administration key string. Use the **no** form to restore the default setting.

Syntax

lacp admin-key *key*
[**no**] **lacp admin-key**

key - The port channel admin key is used to identify a specific link aggregation group (LAG) during local LACP setup on this switch. (Range: 0-65535)

Default Setting

0

Command Mode

Interface Configuration (Port Channel)

Command Usage

- Ports are only allowed to join the same LAG if (1) the LACP system priority matches, (2) the LACP port admin key matches, and (3) the LACP port channel key matches (if configured).
- If the port channel admin key (**lacp admin key** - Port Channel) is not set when a channel group is formed (i.e., it has the null value of 0), this key is set to the same value as the port admin key (**lacp admin key** - Ethernet Interface) used by the interfaces that joined the group. Note

Downloaded from www.Manualslib.com manuals search engine

that when the LAG is no longer used, the port channel admin key is reset to 0.

Example

```
Console(config)#interface port channel 1
Console(config-if)#lacp admin-key 3
Console(config-if)#
```

lacp port-priority

This command configures LACP port priority. Use the **no** form to restore the default setting.

Syntax

lacp {**actor** | **partner**} **port-priority** *priority*
no lacp {**actor** | **partner**} **port-priority**

- **actor** - The local side an aggregate link.
- **partner** - The remote side of an aggregate link.
- *priority* - LACP port priority is used to select a backup link. (Range: 0-65535)

Default Setting

32768

Command Mode

Interface Configuration (Ethernet)

Command Usage

- Setting a lower value indicates a higher effective priority.
- If an active port link goes down, the backup port with the highest priority is selected to replace the downed link. However, if two or more ports have the same LACP port priority, the port with the lowest physical port number will be selected as the backup port.
- Once the remote side of a link has been established, LACP operational settings are already in use on that side. Configuring LACP settings for the partner only applys to its administrative state, not its operational

Downloaded from www.Manualslib.com manuals search engine

state, and will only take effect the next time an aggregate link is established with the partner.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor port-priority 128
```

show lacp

This command displays LACP information.

Syntax

show lacp [*port-channel*] {**counters** | **internal** | **neighbors** | **sys-id**}

- *port-channel* - Local identifier for a link aggregation group. (Range: 1-6)
- **counters** - Statistics for LACP protocol messages.
- **internal** - Configuration settings and operational state for local side.
- **neighbors** - Configuration settings and operational state for remote side.
- **sys-id** - Summary of system priority and MAC address for all channel groups.

Default Setting

Port Channel: all

Command Mode

Privileged Exec

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console#show 1 lacp counters
Channel group : 1
-------------------------------------------------------------------------
Eth 1/ 1
-------------------------------------------------------------------------
  LACPDUs Sent : 21
  LACPDUs Received : 21
  Marker Sent : 0
  Marker Received : 0
  LACPDUs Unknown Pkts : 0
  LACPDUs Illegal Pkts : 0
.
.
.
```

Field	Description
LACPDUs Sent	Number of valid LACPDUs transmitted from this channel group.
LACPDUs Received	Number of valid LACPDUs received on this channel group.
Marker Sent	Number of valid Marker PDUs transmitted from this channel group.
Marker Received	Number of valid Marker PDUs received by this channel group.
LACPDUs Unknown Pkts	Number of frames received that either (1) Carry the Slow Protocols Ethernet Type value, but contain an unknown PDU, or (2) are addressed to the Slow Protocols group MAC Address, but do not carry the Slow Protocols Ethernet Type.
LACPDUs Illegal Pkts	Number of frames that carry the Slow Protocols Ethernet Type value, but contain a badly formed PDU or an illegal value of Protocol Subtype.

Downloaded from www.Manualslib.com manuals search engine

```
Console#show 1 lacp internal
Channel group : 1
------------------------------------------------------------------------
Oper Key : 4
Admin Key : 0
Eth 1/1
------------------------------------------------------------------------
  LACPDUs Internal : 30 sec
  LACP System Priority : 32768
  LACP Port Priority : 32768
  Admin Key : 4
  Oper Key : 4
  Admin State : defaulted, aggregation, long timeout, LACP-activity
  Oper State : distributing, collecting, synchronization, aggregation,
               long timeout, LACP-activity
.
.
.
```

Field	Description
Oper Key	Current operational value of the key for the aggregation port.
Admin Key	Current administrative value of the key for the aggregation port.
LACPDUs Internal	Number of seconds before invalidating received LACPDU information.
LACP System Priority	LACP system priority assigned to this port channel.

Downloaded from www.Manualslib.com manuals search engine

Field	Description
LACP Port Priority	LACP port priority assigned to this interface within the channel group.
Admin State, Oper State	Administrative or operational values of the actor's state parameters: • Expired – The actor's receive machine is in the expired state; • Defaulted – The actor's receive machine is using defaulted operational partner information, administratively configured for the partner. • Distributing – If false, distribution of outgoing frames on this link is disabled; i.e., distribution is currently disabled and is not expected to be enabled in the absence of administrative changes or changes in received protocol information. • Collecting – Collection of incoming frames on this link is enabled; i.e., collection is currently enabled and is not expected to be disabled in the absence of administrative changes or changes in received protocol information. • Synchronization – The System considers this link to be IN_SYNC; i.e., it has been allocated to the correct Link Aggregation Group, the group has been associated with a compatible Aggregator, and the identity of the Link Aggregation Group is consistent with the System ID and operational Key information transmitted. • Aggregation – The system considers this link to be aggregatable; i.e., a potential candidate for aggregation. • Long timeout – Periodic transmission of LACPDUs uses a slow transmission rate. • LACP-Activity – Activity control value with regard to this link. (0: Passive; 1: Active)

Downloaded from www.Manualslib.com manuals search engine

```
Console#show 1 lacp neighbors
Channel group 1 neighbors
-------------------------------------------------------------------------
Eth 1/1
-------------------------------------------------------------------------
  Partner Admin System ID : 32768, 00-00-00-00-00-00
  Partner Oper System ID : 32768, 00-00-00-00-00-01
  Partner Admin Port Number : 1
  Partner Oper Port Number : 1
  Port Admin Priority : 32768
  Port Oper Priority : 32768
  Admin Key : 0
  Oper Key : 4
  Admin State : defaulted, distributing, collecting, synchronization,
                long timeout,
  Oper State : distributing, collecting, synchronization, aggregation,
               long timeout, LACP-activity
.
.
.
```

Field	Description
Partner Admin System ID	LAG partner's system ID assigned by the user.
Partner Oper System ID	LAG partner's system ID assigned by the LACP protocol.
Partner Admin Port Number	Current administrative value of the port number for the protocol Partner.
Partner Oper Port Number	Operational port number assigned to this aggregation port by the port's protocol partner.
Port Admin Priority	Current administrative value of the port priority for the protocol partner.
Port Oper Priority	Priority value assigned to this aggregation port by the partner.
Admin Key	Current administrative value of the Key for the protocol partner.
Oper Key	Current operational value of the Key for the protocol partner.
Admin State	Administrative values of the partner's state parameters. (See preceding table.)
Oper State	Operational values of the partner's state parameters. (See preceding table.)

Downloaded from www.Manualslib.com manuals search engine

```
Console#show lacp sysid
Channel group    System Priority    System MAC Address
--------------------------------------------------------------------------------
            1              32768     00-30-F1-8F-2C-A7
            2              32768     00-30-F1-8F-2C-A7
            3              32768     00-30-F1-8F-2C-A7
            4              32768     00-30-F1-8F-2C-A7
            5              32768     00-30-F1-8F-2C-A7
            6              32768     00-30-F1-8F-2C-A7
Console#
```

Field	Description
Channel group	A link aggregation group configured on this switch.
System Priority*	LACP system priority for this channel group.
System MAC Address*	System MAC address.

* The LACP system priority and system MAC address are concatenated to form the LAG system ID.

Address Table Commands

These commands are used to configure the address table for filtering specified addresses, displaying current entries, clearing the table, or setting the aging time.

Command	Function	Mode	Page
mac-address-table static	Maps a static address to a port in a VLAN	GC	3-34
clear mac-address-table dynamic	Removes any learned entries from the forwarding database	PE	3-35
show mac-address-table	Displays entries in the bridge-forwarding database	PE	3-35
mac-address-table aging-time	Sets the aging time of the address table	GC	3-36
show mac-address-table aging-time	Shows the aging time for the address table	PE	3-37

Downloaded from www.Manualslib.com manuals search engine

mac-address-table static

This command maps a static address to a destination port in a VLAN. Use the **no** form to remove an address.

Syntax

mac-address-table static *mac-address* **interface** *interface* **vlan** *vlan-id* [*action*]

no mac-address-table static *mac-address* **vlan** *vlan-id*

- *mac-address* - MAC address.
- *interface*
  - **ethernet** *unit/port*
    - *unit* - This is device 1.
    - *port* - Port number.
  - **port-channel** *channel-id* (Range: 1-6)
- *vlan-id* - VLAN ID (Range: 1-4094)
- *action* -
  - **delete-on-reset** - Assignment lasts until the switch is reset.
  - **permanent** - Assignment is permanent.

Default Setting

No static addresses are defined. The default mode is **permanent**.

Command Mode

Global Configuration

Command Usage

The static address for a host device can be assigned to a specific port within a specific VLAN. Use this command to add static addresses to the MAC Address Table. Static addresses have the following characteristics:

- Static addresses will not be removed from the address table when a given interface link is down.

Downloaded from www.Manualslib.com manuals search engine

- Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table.
- A static address cannot be learned on another port until the address is removed with the **no** form of this command.

Example

```
Console(config)#mac-address-table static 00-e0-29-94-34-de interface
ethernet 1/1 vlan 1 delete-on-reset
```

clear mac-address-table dynamic

This command removes any learned entries from the forwarding database and clears the transmit and receive counts for any static or system configured entries.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#clear mac-address-table dynamic
```

show mac-address-table

This command shows classes of entries in the bridge-forwarding database.

Syntax

show mac-address-table [**address** *mac-address* [*mask*]] [**interface** *interface*] [**vlan** *vlan-id*] [**sort** {**address** | **vlan** | **interface**}]

- *mac-address* - MAC address.
- *mask* - Bits to match in the address.
- *interface*
  - **ethernet** *unit/port*
    - *unit* - This is device 1.

Downloaded from www.Manualslib.com manuals search engine

- *port* - Port number.
- **port-channel** *channel-id* (Range: 1-6)

- *vlan-id* - VLAN ID (Range: 1-4094)
- **sort** - Sort by address, vlan or interface.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- The MAC Address Table contains the MAC addresses associated with each interface. Note that the Type field may include the following types:
  - Learned - Dynamic address entries
  - Permanent - Static entry
  - Delete-on-reset - Static entry to be deleted when system is reset
- The mask should be hexadecimal numbers (representing an equivalent bit mask) in the form xx-xx-xx-xx-xx-xx that is applied to the specified MAC address. Enter hexadecimal numbers, where an equivalent binary bit "0" means to match a bit and "1" means to ignore a bit. For example, a mask of 00-00-00-00-00-00 means an exact match, and a mask of FF-FF-FF-FF-FF-FF means "any."
- The maximum number of address entries is 8191.

Example

```
Console#show mac-address-table
 Interface Mac Address       Vlan Type
 --------- ----------------- ---- -----------------
  Eth 1/ 1 00-e0-29-94-34-de    1 Delete-on-reset
Console#
```

mac-address-table aging-time

This command sets the aging time for entries in the address table. Use the **no** form to restore the default aging time.

Downloaded from www.Manualslib.com manuals search engine

Syntax

mac-address-table aging-time *seconds*
no mac-address-table aging-time

seconds - Aging time. (Range: 10-1000000 seconds; 0 to disable aging)

Default Setting

300 seconds

Command Mode

Global Configuration

Command Usage

The aging time is used to age out dynamically learned forwarding information.

Example

```
Console(config)#mac-address-table aging-time 100
Console(config)#
```

show mac-address-table aging-time

This command shows the aging time for entries in the address table.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show mac-address-table aging-time
 Aging time: 300 sec.
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Spanning Tree Commands

This section includes commands that configure the Spanning Tree Algorithm (STA) globally for the switch, and commands that configure STA for the selected interface.

Command	Function	Mode	Page
spanning-tree	Enables the spanning tree protocol	GC	3-39
spanning-tree mode	Configures STP, RSTP mode	GC	3-39
spanning-tree forward-time	Configures the spanning tree bridge forward time	GC	3-41
spanning-tree hello-time	Configures the spanning tree bridge hello time	GC	3-42
spanning-tree max-age	Configures the spanning tree bridge maximum age	GC	3-42
spanning-tree priority	Configures the spanning tree bridge priority	GC	3-43
spanning-tree path-cost method	Configures the path cost method for RSTP	GC	3-44
spanning-tree transmission-limit	Configures the transmission limit for RSTP	GC	3-45
spanning-tree spanning-disabled	Disables spanning tree for an interface	IC	
spanning-tree cost	Configures the spanning tree path cost of an interface	IC	3-46
spanning-tree port-priority	Configures the spanning tree priority of an interface	IC	3-47
spanning-tree edge-port	Enables fast forwarding for edge ports	IC	3-48
spanning-tree portfast	Sets an interface to fast forwarding	IC	3-49
spanning-tree link-type	Configures the link type for RSTP	IC	3-50
spanning-tree protocol-migration	Re-checks the appropriate BPDU format	PE	3-51
show spanning-tree	Shows spanning tree configuration for the common spanning tree (i.e., overall bridge), a selected interface, or an instance within the multiple spanning tree	PE	3-51

Downloaded from www.Manualslib.com manuals search engine

spanning-tree

This command enables the Spanning Tree Algorithm globally for the switch. Use the **no** form to disable it.

Syntax

[**no**] **spanning-tree**

Default Setting

Spanning tree is enabled.

Command Mode

Global Configuration

Command Usage

The Spanning Tree Algorithm (STA) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STA-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

Example

This example shows how to enable the Spanning Tree Algorithm for the switch:

```
Console(config)#spanning-tree
Console(config)#
```

spanning-tree mode

This command selects the spanning tree mode for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree mode {**stp** | **rstp**}
no spanning-tree mode

Downloaded from www.Manualslib.com manuals search engine

- **stp** - Spanning Tree Protocol (IEEE 802.1D)
- **rstp** - Rapid Spanning Tree Protocol (IEEE 802.1w)

Default Setting

rstp

Command Mode

Global Configuration

Command Usage

- Spanning Tree Protocol

Uses RSTP for the internal state machine, but sends only 802.1D BPDUs.

- This creates one spanning tree instance for the entire network. If multiple VLANs are implemented on a network, the path between specific VLAN members may be inadvertently disabled to prevent network loops, thus isolating group members. When operating multiple VLANs, we recommend selecting the MSTP option.

- Rapid Spanning Tree Protocol

RSTP supports connections to either STP or RSTP nodes by monitoring the incoming protocol messages and dynamically adjusting the type of protocol messages the RSTP node transmits, as described below:

- STP Mode – If the switch receives an 802.1D BPDU after a port's migration delay timer expires, the switch assumes it is connected to an 802.1D bridge and starts using only 802.1D BPDUs.
- RSTP Mode – If RSTP is using 802.1D BPDUs on a port and receives an RSTP BPDU after the migration delay expires, RSTP restarts the migration delay timer and begins using RSTP BPDUs on that port.

Example

The following example configures the switch to use Rapid Spanning Tree:

```
Console(config)#spanning-tree mode rstp
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

spanning-tree forward-time

This command configures the spanning tree bridge forward time globally for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree forward-time *seconds*
no spanning-tree **forward-time**

seconds - Time in seconds. (Range: 4 - 30 seconds)
The minimum value is the higher of 4 or [(max-age / 2) + 1].

Default Setting

15 seconds

Command Mode

Global Configuration

Command Usage

This command sets the maximum time (in seconds) the root device will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to the discarding state; otherwise, temporary data loops might result.

Example

```
Console(config)#spanning-tree forward-time 20
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

spanning-tree hello-time

This command configures the spanning tree bridge hello time globally for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree hello-time *time*
no spanning-tree hello-time

time - Time in seconds. (Range: 1-10 seconds).
The maximum value is the lower of 10 or [(max-age / 2) -1].

Default Setting

2 seconds

Command Mode

Global Configuration

Command Usage

This command sets the time interval (in seconds) at which the root device transmits a configuration message.

Example

```
Console(config)#spanning-tree hello-time 5
Console(config)#
```

spanning-tree max-age

This command configures the spanning tree bridge maximum age globally for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree max-age *seconds*
no spanning-tree max-age

seconds - Time in seconds. (Range: 6-40 seconds)
The minimum value is the higher of 6 or [2 x (hello-time + 1)].
The maximum value is the lower of 40 or [2 x (forward-time - 1)].

Downloaded from www.Manualslib.com manuals search engine

Default Setting

20 seconds

Command Mode

Global Configuration

Command Usage

This command sets the maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network.

Example

```
Console(config)#spanning-tree max-age 40
Console(config)#
```

spanning-tree priority

This command configures the spanning tree priority globally for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree priority *priority*
no spanning-tree priority

priority - Priority of the bridge. (Range: 0 - 65535)
(Range – 0-61440, in steps of 4096; Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440)

Default Setting

32768

Downloaded from www.Manualslib.com manuals search engine

Command Mode

Global Configuration

Command Usage

Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.

Example

```
Console(config)#spanning-tree priority 40000
Console(config)#
```

spanning-tree pathcost method

This command configures the path cost method used for Rapid Spanning Tree. Use the **no** form to restore the default.

Syntax

spanning-tree pathcost method {**long** | **short**}
no spanning-tree pathcost method

- **long** - Specifies 32-bit based values that range from 1-200,000,000.
- **short** - Specifies 16-bit based values that range from 1-65535.

Default Setting

Long method

Command Mode

Global Configuration

Command Usage

The path cost method is used to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. Note that path cost (page 3-46) takes precedence over port priority (page 3-47).

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console(config)#spanning-tree pathcost method long
Console(config)#
```

spanning-tree transmission-limit

This command configures the minimum interval between the transmission of consecutive RSTP BPDUs. Use the **no** form to restore the default.

Syntax

spanning-tree transmission-limit *count*
no spanning-tree transmission-limit

count - The transmission limit in seconds. (Range: 1-10)

Default Setting

3

Command Mode

Global Configuration

Command Usage

This command limits the maximum transmission rate for BPDUs.

Example

```
Console(config)#spanning-tree transmission-limit 4
Console(config)#
```

This command**spanning-tree spanning-disabled**

This command disables the spanning tree algorithm for the specified interface. Use the **no** form to reenable the spanning tree algorithm for the specified interface.

Syntax

[**no**] **spanning-tree spanning-disabled**
Interface Configuration (Ethernet, Port Channel)

Example

Downloaded from www.Manualslib.com manuals search engine

This example disables the spanning tree algorithm for port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree spanning-disabled
Console(config-if)#
```

spanning-tree cost

This command configures the spanning tree path cost for the specified interface. Use the **no** form to restore the default.

Syntax

spanning-tree cost *cost*
no spanning-tree cost

cost - The path cost for the port. (Range: 1-200,000,000))

The recommended range is:

- Ethernet: 200,000-20,000,000
- Fast Ethernet: 20,000-2,000,000
- Gigabit Ethernet: 2,000-200,000

Default Setting

- Ethernet – half duplex: 2,000,000; full duplex: 1,000,000; trunk: 500,000
- Fast Ethernet – half duplex: 200,000; full duplex: 100,000; trunk: 50,000
- Gigabit Ethernet – full duplex: 10,000; trunk: 5,000

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This command is used by the Spanning Tree Algorithm to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media.
- Path cost takes precedence over port priority.
- When the spanning-tree pathcost method (page 3-44) is set to short,

Downloaded from www.Manualslib.com manuals search engine

the maximum value for path cost is 65,535.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree cost 50
Console(config-if)#
```

spanning-tree port-priority

This command configures the priority for the specified interface. Use the **no** form to restore the default.

Syntax

spanning-tree port-priority *priority*
no spanning-tree port-priority

priority - The priority for a port. (Range: 0-240, in steps of 16)

Default Setting

128

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This command defines the priority for the use of a port in the Spanning Tree Algorithm. If the path cost for all ports on a switch are the same, the port with the highest priority (that is, lowest value) will be configured as an active link in the spanning tree.
- Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree port-priority 0
```

Related Commands

spanning-tree cost (3-46)

Downloaded from www.Manualslib.com manuals search engine

spanning-tree edge-port

This command specifies an interface as an edge port. Use the **no** form to restore the default.

Syntax

[**no**] **spanning-tree edge-port**

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- You can enable this option if an interface is attached to a LAN segment that is at the end of a bridged LAN or to an end node. Since end nodes cannot cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying Edge Ports provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to initiate reconfiguration when the interface changes state, and also overcomes other STA-related timeout problems. However, remember that Edge Port should only be enabled for ports connected to an end-node device.
- This command has the same effect as the **spanning-tree portfast**.

Example

```
Console(config)#interface ethernet ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#
```

Related Commands

spanning-tree portfast (3-49)

Downloaded from www.Manualslib.com manuals search engine

spanning-tree portfast

This command sets an interface to fast forwarding. Use the **no** form to disable fast forwarding.

Syntax

[**no**] **spanning-tree portfast**

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This command is used to enable/disable the fast spanning-tree mode for the selected port. In this mode, ports skip the Discarding and Learning states, and proceed straight to Forwarding.
- Since end-nodes cannot cause forwarding loops, they can be passed through the spanning tree state changes more quickly than allowed by standard convergence time. Fast forwarding can achieve quicker convergence for end-node workstations and servers, and also overcome other STA related timeout problems. (Remember that fast forwarding should only be enabled for ports connected to a LAN segment that is at the end of a bridged LAN or for an end-node device.)
- This command is the same as **spanning-tree edge-port**, and is only included for backward compatibility with earlier products. Note that this command may be removed for future software versions.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#bridge-group 1 portfast
Console(config-if)#
```

Related Commands

spanning-tree edge-port (3-48)

Downloaded from www.Manualslib.com manuals search engine

spanning-tree link-type

This command configures the link type for Rapid Spanning Tree. Use the **no** form to restore the default.

Syntax

spanning-tree link-type {**auto** | **point-to-point** | **shared**}
no spanning-tree link-type

- **auto** - Automatically derived from the duplex mode setting.
- **point-to-point** - Point-to-point link.
- **shared** - Shared medium.

Default Setting

auto

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Specify a point-to-point link if the interface can only be connected to exactly one other bridge, or a shared link if it can be connected to two or more bridges.
- When automatic detection is selected, the switch derives the link type from the duplex mode. A full-duplex interface is considered a point-to-point link, while a half-duplex interface is assumed to be on a shared link.
- RSTP only works on point-to-point links between two bridges. If you designate a port as a shared link, RSTP is forbidden.

Example

```
Console(config)#interface ethernet ethernet 1/5
Console(config-if)#spanning-tree link-type point-to-point
```


Downloaded from www.Manualslib.com manuals search engine

spanning-tree protocol-migration

This command re-checks the appropriate BPDU format to send on the selected interface.

Syntax

spanning-tree protocol-migration *interface*

interface

- **ethernet** *unit/port*

- *unit* - This is device 1.
- *port* - Port number.
  - **port-channel** *channel-id* (Range: 1-6)

Command Mode

Privileged Exec

Command Usage

If at any time the switch detects STP BPDUs, including Configuration or Topology Change Notification BPDUs, it will automatically set the selected interface to forced STP-compatible mode. However, you can also use the **spanning-tree protocol-migration** command at any time to manually re-check the appropriate BPDU format to send on the selected interfaces (i.e., RSTP or STP-compatible).

Example

```
Console(config)#interface ethernet ethernet 1/5
Console(config-if)#spanning-tree protocol-migration
Console(config-if)#
```

show spanning-tree

This command shows the configuration for the common spanning tree (CST) or for an instance within the multiple spanning tree (MST).

Syntax

show spanning-tree [*interface* | **mst** *instance_id*]

- *interface*

Downloaded from www.Manualslib.com manuals search engine

- **ethernet** *unit/port*

- *unit* - This is device 1.
- *port* - Port number.
  - **port-channel** *channel-id* (Range: 1-6)

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- Use the **show spanning-tree** command with no parameters to display the spanning tree configuration for the switch and for every interface in the tree.
- Use the **show spanning-tree** *interface* command to display the spanning tree configuration for an interface.
-
- For a description of the items displayed under "Spanning-tree information," see "Configuring Global Settings" on page 3-131. For a description of the items displayed for specific interfaces, see "Displaying Interface Settings" on page 3-136.

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console#show spanning-tree
Spanning-tree information
----------------------------------------------------------------
Spanning-tree information
----------------------------------------------------------------
 Spanning tree mode               :MSTP
 Spanning tree enable/disable     :enable
 Instance                         :0
 Vlans configuration              :1-4094
 Priority                         :32768
 Bridge Hello Time (sec.)         :2
 Bridge Max Age (sec.)            :20
 Bridge Forward Delay (sec.)      :15
 Root Hello Time (sec.)           :2
 Root Max Age (sec.)              :20
 Root Forward Delay (sec.)        :15
 Max hops                         :20
 Remaining hops                   :20
 Designated Root                  :32768.0.0000ABCD0000
 Current root port                :1
 Current root cost                :200000
 Number of topology changes       :1
 Last topology changes time (sec.):22
 Transmission limit               :3
 Path Cost Method                 :long
----------------------------------------------------------------
Eth  1/ 1 information
----------------------------------------------------------------
Admin status         : enable
 Role                 : root
 State                : forwarding
 External path cost   : 100000
 Internal path cost   : 100000
 Priority             : 128
 Designated cost      : 200000
 Designated port      : 128.24
 Designated root      : 32768.0.0000ABCD0000
 Designated bridge    : 32768.0.0030F1552000
 Fast forwarding      : disable
 Forward transitions  : 1
 Admin edge port      : enable
 Oper edge port       : disable
 Admin Link type      : auto
 Oper Link type       : point-to-point
 Spanning Tree Status : enable
.
.
.
Console#
```


Downloaded from www.Manualslib.com manuals search engine

VLAN Commands

A VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment. This section describes commands used to create VLAN groups, add port members, specify how VLAN tagging is used, and enable automatic VLAN registration for the selected interface.

Command Groups	Function	Page
Editing VLAN Groups	Sets up VLAN groups, including name, VID and state	3-54
Configuring VLAN Interfaces	Configures VLAN interface parameters, including ingress and egress tagging mode, ingress filtering, PVID, and GVRP	3-57
Displaying VLAN Information	Displays VLAN groups, status, port members, and MAC addresses	3-64
Configuring Protocol VLANs	Configures protocol-based VLANs based on frame type and protocol	3-65
Configuring Private VLANs	Configures private VLANs, including uplink and downlink ports	3-70

Editing VLAN Groups

Command	Function	Mode	Page
vlan database	Enters VLAN database mode to add, change, and delete VLANs	GC	3-54
vlan	Configures a VLAN, including VID, name and state	VC	3-55

vlan database

This command enters VLAN database mode. All commands in this mode will take effect immediately.

Default Setting

None

Downloaded from www.Manualslib.com manuals search engine

Command Mode

Global Configuration

Command Usage

- Use the VLAN database command mode to add, change, and delete VLANs. After finishing configuration changes, you can display the VLAN settings by entering the **show vlan** command.
- Use the **interface vlan** command mode to define the port membership mode and add or remove ports from a VLAN. The results of these commands are written to the running-configuration file, and you can display this file by entering the **show running-config** command.

Example

```
Console(config)#vlan database
Console(config-vlan)#
```

Related Commands

show vlan (3-64)

vlan

This command configures a VLAN. Use the **no** form to restore the default settings or delete a VLAN.

Syntax

vlan *vlan-id* [**name** *vlan-name*] **media ethernet** [**state** {**active** | **suspend**}]
no vlan *vlan-id* [**name** | **state**]

- *vlan-id* - ID of configured VLAN. (Range: 1-4094, no leading zeroes)
- **name** - Keyword to be followed by the VLAN name.
  - *vlan-name* - ASCII string from 1 to 32 characters.
- **media ethernet** - Ethernet media type.
- **state** - Keyword to be followed by the VLAN state.
  - **active** - VLAN is operational.

Downloaded from www.Manualslib.com manuals search engine

- **suspend** - VLAN is suspended. Suspended VLANs do not pass packets.

Default Setting

By default only VLAN 1 exists and is active.

Command Mode

VLAN Database Configuration

Command Usage

- **no vlan** *vlan-id* deletes the VLAN.
- **no vlan** *vlan-id* **name** removes the VLAN name.
- **no vlan** *vlan-id* **state** returns the VLAN to the default state (i.e., active).
- You can configure up to 255 VLANs on the switch.

Example

The following example adds a VLAN, using VLAN ID 105 and name RD5. The VLAN is activated by default.

```
Console(config)#vlan database
Console(config-vlan)#vlan 105 name RD5 media ethernet
Console(config-vlan)#
```

Related Commands

show vlan (3-64)

Downloaded from www.Manualslib.com manuals search engine

Configuring VLAN Interfaces

Command	Function	Mode	Page
interface vlan	Enters interface configuration mode for a specified VLAN	IC	3-57
switchport mode	Configures VLAN membership mode for an interface	IC	3-58
switchport acceptable-frame-types	Configures frame types to be accepted by an interface	IC	3-59
switchport ingress-filtering	Enables ingress filtering on an interface	IC	3-60
switchport native vlan	Configures the PVID (native VLAN) of an interface	IC	3-61
switchport allowed vlan	Configures the VLANs associated with an interface	IC	3-62
switchport gvrp	Enables GVRP for an interface	IC	3-73
switchport forbidden vlan	Configures forbidden VLANs for an interface	IC	3-63

interface vlan

This command enters interface configuration mode for VLANs, which is used to configure VLAN parameters for a physical interface.

Syntax

interface vlan *vlan-id*

vlan-id - ID of the configured VLAN. (Range: 1-4094, no leading zeroes)

Default Setting

None

Command Mode

Global Configuration

Downloaded from www.Manualslib.com manuals search engine

Example

The following example shows how to set the interface configuration mode to VLAN 1, and then assign an IP address to the VLAN:

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.254 255.255.255.0
Console(config-if)#
```

Related Commands

shutdown (3-9)

switchport mode

This command configures the VLAN membership mode for a port. Use the **no** form to restore the default.

Syntax

switchport mode {**trunk** | **hybrid**}
no switchport mode

- **trunk** - Specifies a port as an end-point for a VLAN trunk. A trunk is a direct link between two switches, so the port transmits tagged frames that identify the source VLAN. However, note that frames belonging to the port's default VLAN (i.e., associated with the PVID) are sent untagged.
- **hybrid** - Specifies a hybrid VLAN interface. The port may transmit tagged or untagged frames.

Default Setting

All ports are in hybrid mode with the PVID set to VLAN 1.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Downloaded from www.Manualslib.com manuals search engine

Example

The following shows how to set the configuration mode to port 1, and then set the switchport mode to hybrid:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport mode hybrid
Console(config-if)#
```

Related Commands

switchport acceptable-frame-types (3-59)

switchport acceptable-frame-types

This command configures the acceptable frame types for a port. Use the **no** form to restore the default.

Syntax

switchport acceptable-frame-types {**all** | **tagged**}
no switchport acceptable-frame-types

- **all** - The port accepts all frames, tagged or untagged.
- **tagged** - The port only receives tagged frames.

Default Setting

All frame types

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

When set to receive all frame types, any received frames that are untagged are assigned to the default VLAN.

Downloaded from www.Manualslib.com manuals search engine

Example

The following example shows how to restrict the traffic received on port 1 to tagged frames:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport acceptable-frame-types tagged
Console(config-if)#
```

Related Commands

switchport mode (3-58)

switchport ingress-filtering

This command enables ingress filtering for an interface. Use the **no** form to restore the default.

Syntax

[**no**] **switchport ingress-filtering**

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Ingress filtering only affects tagged frames.
- If ingress filtering is disabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be flooded to all other ports (except for those VLANs explicitly forbidden on this port).
- If ingress filtering is enabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be discarded.
- Ingress filtering does not affect VLAN independent BPDU frames, such as GVRP or STA. However, they do affect VLAN dependent BPDU frames, such as GMRP.

Downloaded from www.Manualslib.com manuals search engine

Example

The following example shows how to set the interface to port 1 and then enable ingress filtering:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport ingress-filtering
Console(config-if)#
```

switchport native vlan

This command configures the PVID (i.e., default VLAN ID) for a port. Use the **no** form to restore the default.

Syntax

switchport native vlan *vlan-id*
no switchport native vlan

vlan-id - Default VLAN ID for a port. (Range: 1-4094, no leading zeroes)

Default Setting

VLAN 1

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- If an interface is not a member of VLAN 1 and you assign its PVID to this VLAN, the interface will automatically be added to VLAN 1 as an untagged member. For all other VLANs, an interface must first be configured as an untagged member before you can assign its PVID to that group.
- If acceptable frame types is set to **all** or switchport mode is set to **hybrid**, the PVID will be inserted into all untagged frames entering the ingress port.

Downloaded from www.Manualslib.com manuals search engine

Example

The following example shows how to set the PVID for port 1 to VLAN 3:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport native vlan 3
Console(config-if)#
```

switchport allowed vlan

This command configures VLAN groups on the selected interface. Use the **no** form to restore the default.

Syntax

switchport allowed vlan {**add** *vlan-list* [**tagged** | **untagged**] | **remove** *vlan-list*}

no switchport allowed vlan

- **add** *vlan-list* - List of VLAN identifiers to add.
- **remove** *vlan-list* - List of VLAN identifiers to remove.
- *vlan-list* - Separate nonconsecutive VLAN identifiers with a comma and no spaces; use a hyphen to designate a range of IDs. Do not enter leading zeros. (Range: 1-4094).

Default Setting

All ports are assigned to VLAN 1 by default.
The default frame type is untagged.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- A port, or a trunk with switchport mode set to **hybrid**, must be assigned to at least one VLAN as untagged.
- If a trunk has switchport mode set to **trunk** (i.e., 1Q Trunk), then you can only assign an interface to VLAN groups as a tagged member.
- Frames are always tagged within the switch. The tagged/untagged parameter used when adding a VLAN to an interface tells the switch

Downloaded from www.Manualslib.com manuals search engine

whether to keep or remove the tag from a frame on egress.

- If none of the intermediate network devices nor the host at the other end of the connection supports VLANs, the interface should be added to these VLANs as an untagged member. Otherwise, it is only necessary to add at most one VLAN as untagged, and this should correspond to the native VLAN for the interface.
- If a VLAN on the forbidden list for an interface is manually added to that interface, the VLAN is automatically removed from the forbidden list for that interface.

Example

The following example shows how to add VLANs 1, 2, 5 and 6 to the allowed list as tagged VLANs for port 1:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport allowed vlan add 1,2,5,6 tagged
Console(config-if)#
```

switchport forbidden vlan

This command configures forbidden VLANs. Use the **no** form to remove the list of forbidden VLANs.

Syntax

switchport forbidden vlan {**add** *vlan-list* | **remove** *vlan-list*}
no switchport forbidden vlan

- **add** *vlan-list* - List of VLAN identifiers to add.
- **remove** *vlan-list* - List of VLAN identifiers to remove.
- *vlan-list* - Separate nonconsecutive VLAN identifiers with a comma and no spaces; use a hyphen to designate a range of IDs. Do not enter leading zeros. (Range: 1-4094).

Default Setting

No VLANs are included in the forbidden list.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Downloaded from www.Manualslib.com manuals search engine

Command Usage

- This command prevents a VLAN from being automatically added to the specified interface via GVRP.
- If a VLAN has been added to the set of allowed VLANs for an interface, then you cannot add it to the set of forbidden VLANs for that same interface.

Example

The following example shows how to prevent port 1 from being added to VLAN 3:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport forbidden vlan add 3
Console(config-if)#
```

Displaying VLAN Information

Command	Function	Mode	Page
show vlan	Shows VLAN information	NE, PE	3-64
show interfaces status vlan	Displays status for the specified VLAN interface	NE, PE	3-11
show interfaces switchport	Displays the administrative and operational status of an interface	NE, PE	3-14

show vlan

This command shows VLAN information.

Syntax

show vlan [**id** *vlan-id* | **name** *vlan-name*]

- **id** - Keyword to be followed by the VLAN ID.
  - *vlan-id* - ID of the configured VLAN. (Range: 1-4094, no leading zeroes)
- **name** - Keyword to be followed by the VLAN name.
  - *vlan-name* - ASCII string from 1 to 32 characters.

Downloaded from www.Manualslib.com manuals search engine

Default Setting

Shows all VLANs.

Command Mode

Normal Exec, Privileged Exec

Example

The following example shows how to display information for VLAN 1:

```
Console#show vlan id 1
VLAN Type    Name              Status    Ports/Channel groups
---- ------- ----------------- --------- -----------------------------------
   1 Static     DefaultVlan    Active Eth1/ 1 Eth1/ 2 Eth1/ 3 Eth1/ 4 Eth1/ 5
                                      Eth1/ 6 Eth1/ 7 Eth1/ 8 Eth1/ 9 Eth1/10
                                          Eth1/11 Eth1/12
Console#
```

Configuring Protocol-based VLANs

The network devices required to support multiple protocols cannot be easily grouped into a common VLAN. This may require non-standard devices to pass traffic between different VLANs in order to encompass all the devices participating in a specific protocol. This kind of configuration deprives users of the basic benefits of VLANs, including security and easy accessibility.

To avoid these problems, you can configure this switch with protocol-based VLANs that divide the physical network into logical VLAN groups for each required protocol. When a frame is received at a port, its VLAN membership can then be determined based on the protocol type in use by the inbound packets.

Command	Function	Mode	Page
protocol-vlan protocol-group	Create a protocol group, specifying the supported protocols	GC	3-66
protocol-vlan protocol-group	Maps a protocol group to a VLAN	IC	3-67

Downloaded from www.Manualslib.com manuals search engine

Command	Function	Mode	Page
show protocol-vlan protocol-group	Shows the configuration of protocol groups	PE	3-68
show interfaces protocol-vlan protocol-group	Shows the interfaces mapped to a protocol group and the corresponding VLAN	PE	3-69

To configure protocol-based VLANs, follow these steps:

1. First configure VLAN groups for the protocols you want to use (page 3-55). Although not mandatory, we suggest configuring a separate VLAN for each major protocol running on your network. Do not add port members at this time.
2. Create a protocol group for each of the protocols you want to assign to a VLAN using the **protocol-vlan protocol-group** command (General Configuration mode).
3. Then map the protocol for each interface to the appropriate VLAN using the **protocol-vlan protocol-group** command (Interface Configuration mode).

protocol-vlan protocol-group (Configuring Groups)

This command creates a protocol group, or to add specific protocols to a group. Use the **no** form to remove a protocol group.

Syntax

protocol-vlan protocol-group *group-id* [{**add** | **remove**} **frame-type** *frame* **protocol-type** *protocol*]

no protocol-vlan protocol-group *group-id*

- *group-id* - Group identifier of this protocol group. (Range: 1-2147483647)
- *frame* - Frame type used by this protocol. (Options: ethernet, rfc_1042, snap_8021h, snap_other, llc_other)
- *protocol* - Protocol type. The only option for the llc_other frame type is ipx_raw. The options for all other frames types include: ip, arp,

Downloaded from www.Manualslib.com manuals search engine

rarp.

Default Setting

No protocol groups are configured.

Command Mode

Global Configuration

Example

The following creates protocol group 1, and specifies Ethernet frames with IP and ARP protocol types:

```
Console(config)#protocol-vlan protocol-group 1 add frame-type ethernet
protocol-type ip
Console(config)#protocol-vlan protocol-group 1 add frame-type ethernet
protocol-type arp
Console(config)#
```

protocol-vlan protocol-group (Configuring Interfaces)

This command maps a protocol group to a VLAN for the current interface. Use the **no** form to remove the protocol mapping for this interface.

Syntax

protocol-vlan protocol-group *group-id* **vlan** *vlan-id*
no protocol-vlan protocol-group *group-id* **vlan**

- *group-id* - Group identifier of this protocol group. (Range: 1-2147483647)
- *vlan-id* - VLAN to which matching protocol traffic is forwarded. (Range: 1-4094)

Default Setting

No protocol groups are mapped for any interface.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Downloaded from www.Manualslib.com manuals search engine

Command Usage

- When creating a protocol-based VLAN, only assign interfaces via this command. If you assign interfaces using any of the other VLAN commands (such as **vlan** on page 3-55), these interfaces will admit traffic of any protocol type into the associated VLAN.
- When a frame enters a port that has been assigned to a protocol VLAN, it is processed in the following manner:
  - If the frame is tagged, it will be processed according to the standard rules applied to tagged frames.
  - If the frame is untagged and the protocol type matches, the frame is forwarded to the appropriate VLAN.
  - If the frame is untagged but the protocol type does not match, the frame is forwarded to the default VLAN for this interface.

Example

The following example maps the traffic entering Port 1 which matches the protocol type specified in protocol group 1 to VLAN 2.

```
Console(config)#interface ethernet 1/1
Console(config-if)#protocol-vlan protocol-group 1 vlan 2
Console(config-if)#
```

show protocol-vlan protocol-group

This command shows the frame and protocol type associated with protocol groups.

Syntax

show protocol-vlan protocol-group [*group-id*]

group-id - Group identifier for a protocol group. (Range: 1-2147483647)

Default Setting

All protocol groups are displayed.

Downloaded from www.Manualslib.com manuals search engine

Command Mode

Privileged Exec

Example

This shows protocol group 1 configured for IP over Ethernet:

```
Console#show protocol-vlan protocol-group

 ProtocolGroup ID   Frame Type    Protocol Type
------------------ ------------- ---------------
                1      ethernet     08 00
Console#
```

show interfaces protocol-vlan protocol-group

This command shows the mapping from protocol groups to VLANs for the selected interfaces.

Syntax

show interfaces protocol-vlan protocol-group [*interface*]

interface

- **ethernet** *unit/port*
  - *unit* - This is device 1.
  - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-6)

Default Setting

The mapping for all interfaces is displayed.

Command Mode

Privileged Exec

Downloaded from www.Manualslib.com manuals search engine

Example

This shows that traffic entering Port 1 that matches the specifications for protocol group 1 will be mapped to VLAN 2:

```
Console#show interfaces protocol-vlan protocol-group

   Port     ProtocolGroup ID    Vlan ID
---------- ------------------ -----------
   Eth 1/1                  1       vlan2
Console#
```

Configuring Private VLANs

Private VLANs provide port-based security and isolation between ports within the assigned VLAN. This section describes commands used to configure private VlANs.

Command	Function	Mode	Page
pvlan	Enables and configured private VLANS	GC	3-70
show pvlan	Displays the configured private VLANS	PE	3-71

pvlan

This command enables or configures a private VLAN. Use the **no** form to disable the private VLAN.

Syntax

pvlan [**up-link** *interface-list* **down-link** *interface-list*]
no pvlan

- **up-link** – Specifies an uplink interface.
- **down-link** – Specifies a downlink interface.

Default Setting

No private VLANs are defined.

Command Mode

Global Configuration

Downloaded from www.Manualslib.com manuals search engine

Command Usage

- A private VLAN provides port-based security and isolation between ports within the VLAN. Data traffic on the downlink ports can only be forwarded to, and from, the uplink port.
- Private VLANs and normal VLANs can exist simultaneously within the same switch.
- Entering the **pvlan** command without any parameters enables the private VLAN. Entering **no pvlan** disables the private VLAN.

Example

This example enables the private VLAN, and then sets port 12 as the uplink and ports 1-8 as the downlinks.

```
Console(config)#pvlan
Console(config)#pvlan up-link ethernet 1/12 down-link ethernet 1/1-8
Console(config)#
```

show pvlan

This command displays the configured private VLAN.

Command Mode

Privileged Exec

Example

```
Console#show pvlan
Private VLAN status: Enabled
Up-link port:
 Ethernet 1/12
Down-link port:
 Ethernet 1/1-8
Console#
```

GVRP and Bridge Extension Commands

GARP VLAN Registration Protocol defines a way for switches to exchange VLAN information in order to automatically register VLAN members on interfaces across the network. This section describes how to enable GVRP for individual interfaces and globally for the switch, as well

Downloaded from www.Manualslib.com manuals search engine

as how to display default configuration settings for the Bridge Extension MIB.

Command	Function	Mode	Page
bridge-ext gvrp	Enables GVRP globally for the switch	GC	3-72
show bridge-ext	Shows the global bridge extension configuration	PE	3-73
switchport gvrp	Enables GVRP for an interface	IC	3-73
switchport forbidden vlan	Configures forbidden VLANs for an interface	IC	3-63
show gvrp configuration	Displays GVRP configuration for the selected interface	NE, PE	3-74
garp timer	Sets the GARP timer for the selected function	IC	3-75
show garp timer	Shows the GARP timer for the selected function	NE, PE	3-76

bridge-ext gvrp

This command enables GVRP globally for the switch. Use the **no** form to disable it.

Syntax

[**no**] **bridge-ext gvrp**

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

GVRP defines a way for switches to exchange VLAN information in order to register VLAN members on ports across the network. This function should be enabled to permit automatic VLAN registration, and to support VLANs which extend beyond the local switch.

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console(config)#bridge-ext gvrp
Console(config)#
```

show bridge-ext

This command shows the configuration for bridge extension commands.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

See "Displaying Basic VLAN Information" on page 3-154 and "Displaying Bridge Extension Capabilities" on page 3-18 for a description of the displayed items.

Example

```
Console#show bridge-ext
 Max support vlan numbers: 255
 Max support vlan ID: 4094
 Extended multicast filtering services: No
 Static entry individual port: Yes
 VLAN learning: IVL
 Configurable PVID tagging: Yes
 Local VLAN capable: Yes
 Traffic classes: Enabled
 Global GVRP status: Disabled
 GMRP: Disabled
Console#
```

switchport gvrp

This command enables GVRP for a port. Use the **no** form to disable it.

Syntax

[**no**] **switchport gvrp**

Downloaded from www.Manualslib.com manuals search engine

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport gvrp
Console(config-if)#
```

show gvrp configuration

This command shows if GVRP is enabled.

Syntax

show gvrp configuration [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - This is device 1.
  - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-6)

Default Setting

Shows both global and interface-specific configuration.

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show gvrp configuration ethernet 1/7
Eth 1/ 7:
 Gvrp configuration: Disabled
Console#
```


Downloaded from www.Manualslib.com manuals search engine

garp timer

This command sets the values for the join, leave and leaveall timers. Use the **no** form to restore the timers' default values.

Syntax

garp timer {**join** | **leave** | **leaveall**} *timer_value*
no garp timer {**join** | **leave** | **leaveall**}

- {**join** | **leave** | **leaveall**} - Which timer to set.
- *timer_value* - Value of timer.
  Ranges:
  join: 20-1000 centiseconds
  leave: 60-3000 centiseconds
  leaveall: 500-18000 centiseconds

Default Setting

- join: 20 centiseconds
- leave: 60 centiseconds
- leaveall: 1000 centiseconds

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Group Address Registration Protocol is used by GVRP and GMRP to register or deregister client attributes for client services within a bridged LAN. The default values for the GARP timers are independent of the media access method or data rate. These values should not be changed unless you are experiencing difficulties with GMRP or GVRP registration/deregistration.
- Timer values are applied to GVRP for all the ports on all VLANs.
- Timer values must meet the following restrictions:
  - leave >= (2 x join)
  - leaveall > leave

Note: Set GVRP timers on all Layer 2 devices connected in the same network to the same values. Otherwise, GVRP may not operate

Downloaded from www.Manualslib.com manuals search engine

successfully.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#garp timer join 100
Console(config-if)#
```

Related Commands

show garp timer (3-76)

show garp timer

This command shows the GARP timers for the selected interface.

Syntax

show garp timer [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - This is device 1.
  - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-6)

Default Setting

Shows all GARP timers.

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show garp timer ethernet 1/1
Eth 1/ 1 GARP timer status:
 Join timer: 20 centiseconds
 Leave timer: 60 centiseconds
 Leaveall timer: 1000 centiseconds
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Related Commands

garp timer (3-75)

Priority Commands

The commands described in this section allow you to specify which data packets have greater precedence when traffic is buffered in the switch due to congestion. This switch supports CoS with eight priority queues for each port. Data packets in a port's high-priority queue will be transmitted before those in the lower-priority queues. You can set the default priority

Downloaded from www.Manualslib.com manuals search engine

for each interface, the relative weight of each queue, and the mapping of frame priority tags to the switch's priority queues.

Command Groups	Function	Page
Priority (Layer 2)	Configures default priority for untagged frames, sets queue weights, and maps class of service tags to hardware queues	3-78
Priority (Layer 3 and 4)	Maps TCP ports, IP precedence tags, or IP DSCP tags to class of service values	3-85

Priority Commands (Layer 2)

Command	Function	Mode	Page
switchport priority default	Sets a port priority for incoming untagged frames	IC	3-78
queue mode	Sets the queue mode to strict priority or Weighted Round-Robin (WRR)	GC	3-80
queue bandwidth	Assigns round-robin weights to the priority queues	GC	3-81
queue cos map	Assigns class-of-service values to the priority queues	IC	3-81
show queue mode	Shows the current queue mode	PE	3-83
show queue bandwidth	Shows round-robin weights assigned to the priority queues	PE	3-84
show queue cos-map	Shows the class-of-service map	PE	3-84
show interfaces switchport	Displays the administrative and operational status of an interface	PE	3-14

switchport priority default

This command sets a priority for incoming untagged frames. Use the **no** form to restore the default value.

Syntax

switchport priority default *default-priority-id*
no switchport priority default

Downloaded from www.Manualslib.com manuals search engine

default-priority-id - The priority number for untagged ingress traffic. The priority is a number from 0 to 7. Seven is the highest priority.

Default Setting

The priority is not set, and the default value for untagged frames received on the interface is zero.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
- The default priority applies for an untagged frame received on a port set to accept all frame types (i.e, receives both untagged and tagged frames). This priority does not apply to IEEE 802.1Q VLAN tagged frames. If the incoming frame is an IEEE 802.1Q VLAN tagged frame, the IEEE 802.1p User Priority bits will be used.
- This switch provides eight priority queues for each port. It is configured to use Weighted Round Robin, which can be viewed with the **show queue bandwidth** command. Inbound frames that do not have VLAN tags are tagged with the input port's default ingress user priority, and then placed in the appropriate priority queue at the output port. The default priority for all ingress ports is zero. Therefore, any inbound frames that do not have priority tags will be placed in queue 0 of the output port. (Note that if the output port is an untagged member of the associated VLAN, these frames are stripped of all VLAN tags prior to transmission.)

Example

The following example shows how to set a default priority on port 3 to 5:

```
Console(config)#interface ethernet 1/3
Console(config-if)#switchport priority default 5
```


Downloaded from www.Manualslib.com manuals search engine

queue mode

This command sets the queue mode to strict priority or Weighted Round-Robin (WRR) for the class of service (CoS) priority queues. Use the **no** form to restore the default value.

Syntax

queue mode {**strict** | **wrr**}
no queue mode

- **strict** - Services the egress queues in sequential order, transmitting all traffic in the higher priority queues before servicing lower priority queues.
- **wrr** - Weighted Round-Robin shares bandwidth at the egress ports by using scheduling weights 1, 2, 4, 6, 8, 10, 12, 14 for queues 0 - 7 respectively.

Default Setting

Weighted Round Robin

Command Mode

Global Configuration

Command Usage

You can set the switch to service the queues based on a strict rule that requires all traffic in a higher priority queue to be processed before lower priority queues are serviced, or use Weighted Round-Robin (WRR) queuing that specifies a relative weight of each queue. WRR uses a predefined relative weight for each queue that determines the percentage of service time the switch services each queue before moving on to the next queue. This prevents the head-of-line blocking that can occur with strict priority queuing.

Example

The following example sets the queue mode to strict priority service mode:

```
Console(config)#queue mode strict
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

queue bandwidth

This command assigns weighted round-robin (WRR) weights to the eight class of service (CoS) priority queues. Use the **no** form to restore the default weights.

Syntax

queue bandwidth *weight1...weight4*
no queue bandwidth

weight1...weight4 - The ratio of weights for queues 0 - 3 determines the weights used by the WRR scheduler. (Range: 1 - 15)

Default Setting

Weights 1, 2, 4, 6, 8, 10, 12, 14 are assigned to queues 0 - 7 respectively.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

WRR controls bandwidth sharing at the egress port by defining scheduling weights.

Example

This example shows how to assign WRR weights to each of the priority queues:

```
Console(config)#queue bandwidth 1 3 5 7 9 11 13 15
Console(config)#
```

Related Commands

show queue bandwidth (3-84)

queue cos-map

This command assigns class of service (CoS) values to the priority queues (i.e., hardware output queues 0 - 7). Use the **no** form set the CoS map to the default values.

Downloaded from www.Manualslib.com manuals search engine

Syntax

queue cos-map *queue_id* [*cos1 ... cosn*]
no queue cos-map

- *queue_id* - The ID of the priority queue.
  Ranges are 0 to 7, where 7 is the highest priority queue.
- *cos1 .. cosn* - The CoS values that are mapped to the queue ID. It is a space-separated list of numbers. The CoS value is a number from 0 to 7, where 7 is the highest priority.

Default Setting

This switch supports Class of Service by using eight priority queues, with Weighted Round Robin queuing for each port. Eight separate traffic classes are defined in IEEE 802.1p. The default priority levels are assigned according to recommendations in the IEEE 802.1p standard as shown below.

Queue	0	1	2	3	4	5	6	7
Priority	2	0	1	3	4	5	6	7

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- CoS values assigned at the ingress port are also used at the egress port.
- This command sets the CoS priority for all interfaces.

Downloaded from www.Manualslib.com manuals search engine

Example

The following example shows how to change the CoS assignments to a one-to-one mapping:

```
Console(config)#interface ethernet 1/1
Console(config-if)#queue cos-map 0 0
Console(config-if)#queue cos-map 1 1
Console(config-if)#queue cos-map 2 2
Console(config-if)#exit
Console#show queue cos-map ethernet 1/1
Information of Eth 1/1
 Traffic Class : 0 1 2 3 4 5 6 7
 Priority Queue: 0 1 2 3 4 5 6 7
Information of Eth 1/2
 Traffic Class : 0 1 2 3 4 5 6 7
 Priority Queue: 0 1 2 3 4 5 6 7
.
.
.
```

Related Commands

show queue cos-map (3-84)

show queue mode

This command shows the current queue mode.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#sh queue mode

Wrr status: Enabled
Console#
```


Downloaded from www.Manualslib.com manuals search engine

show queue bandwidth

This command displays the weighted round-robin (WRR) bandwidth allocation for the eight priority queues.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show queue bandwidth
Information of Eth 1/1
 Queue ID  Weight
 --------  ------
    0        1
    1        2
    2        4
    3        6
    4        8
    5        10
    6        12
    7        14
.
.
.
Console#
```

show queue cos-map

This command shows the class of service priority map.

Syntax

show queue cos-map [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - This is device 1.
  - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-6)

Downloaded from www.Manualslib.com manuals search engine

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show queue cos-map ethernet 1/1
Information of Eth 1/1
 CoS Value     : 0 1 2 3 4 5 6 7
 Priority Queue: 2 0 1 3 4 5 6 7
Console#
```

Priority Commands (Layer 3 and 4)

Command	Function	Mode	Page
map ip port	Enables TCP/UDP class of service mapping	GC	3-85
map ip port	Maps TCP/UDP socket to a class of service	IC	3-87
map ip precedence	Enables IP precedence class of service mapping	GC	3-88
map ip precedence	Maps IP precedence value to a class of service	IC	3-88
map ip dscp	Enables IP DSCP class of service mapping	GC	3-89
map ip dscp	Maps IP DSCP value to a class of service	IC	3-90
show map ip port	Shows the IP port map	PE	3-91
show map ip precedence	Shows the IP precedence map	PE	3-92
show map ip dscp	Shows the IP DSCP map	PE	3-93

map ip port (Global Configuration)

Use this command to enable IP port mapping (i.e., class of service mapping for TCP/UDP sockets). Use the **no** form to disable IP port mapping.

Syntax

[**no**] **map ip port**

Downloaded from www.Manualslib.com manuals search engine

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.

Example

The following example shows how to enable TCP/UDP port mapping globally:

```
Console(config)#map ip port
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

map ip port (Interface Configuration)

Use this command to set IP port priority (i.e., TCP/UDP port priority). Use the **no** form to remove a specific setting.

Syntax

map ip port *port-number* **cos** *cos-value*
no map ip port *port-number*

- *port-number* - 16-bit TCP/UDP port number. (Range: 0-65535)
- *cos-value* - Class-of-Service value (Range: 0-7)

Default Setting

None

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
- This command sets the IP port priority for all interfaces.

Example

The following example shows how to map HTTP traffic to CoS value 0:

```
Console(config)#interface ethernet 1/5
Console(config-if)#map ip port 80 cos 0
Console(config-if)#
```


Downloaded from www.Manualslib.com manuals search engine

map ip precedence (Global Configuration)

This command enables IP precedence mapping (i.e., IP Type of Service). Use the **no** form to disable IP precedence mapping.

Syntax

[**no**] **map ip precedence**

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
- IP Precedence and IP DSCP cannot both be enabled. Enabling one of these priority types will automatically disable the other type.

Example

The following example shows how to enable IP precedence mapping globally:

```
Console(config)#map ip precedence
Console(config)#
```

map ip precedence (Interface Configuration)

This command sets IP precedence priority (i.e., IP Type of Service priority). Use the **no** form to restore the default table.

Syntax

map ip precedence *ip-precedence-value* **cos** *cos-value*
no map ip precedence

- *precedence-value* - 3-bit precedence value. (Range: 0-7)
- *cos-value* - Class-of-Service value (Range: 0-7)

Downloaded from www.Manualslib.com manuals search engine

Default Setting

The list below shows the default priority mapping.

IP Precedence Value	0	1	2	3	4	5	6	7
CoS Value	0	1	2	3	4	5	6	7

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
- IP Precedence values are mapped to default Class of Service values on a one-to-one basis according to recommendations in the IEEE 802.1p standard, and then subsequently mapped to the eight hardware priority queues.
- This command sets the IP Precedence for all interfaces.

Example

The following example shows how to map IP precedence value 1 to CoS value 0:

```
Console(config)#interface ethernet 1/5
Console(config-if)#map ip precedence 1 cos 0
Console(config-if)#
```

map ip dscp (Global Configuration)

This command enables IP DSCP mapping (i.e., Differentiated Services Code Point mapping). Use the **no** form to disable IP DSCP mapping.

Syntax

[**no**] **map ip dscp**

Default Setting

Disabled

Downloaded from www.Manualslib.com manuals search engine

Command Mode

Global Configuration

Command Usage

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
- IP Precedence and IP DSCP cannot both be enabled. Enabling one of these priority types will automatically disable the other type.

Example

The following example shows how to enable IP DSCP mapping globally:

```
Console(config)#map ip dscp
Console(config)#
```

map ip dscp (Interface Configuration)

This command sets IP DSCP priority (i.e., Differentiated Services Code Point priority). Use the **no** form to restore the default table.

Syntax

map ip dscp *dscp-value* **cos** *cos-value*
no map ip dscp

- *dscp-value* - 8-bit DSCP value. (Range: 0-255)
- *cos-value* - Class-of-Service value (Range: 0-7)

Default Setting

The DSCP default values are defined in the following table. Note that all the DSCP values that are not specified are mapped to CoS value 0.

IP DSCP Value	CoS Value
0	0
8	1
10, 12, 14, 16	2
18, 20, 22, 24	3
26, 28, 30, 32, 34, 36	4

Downloaded from www.Manualslib.com manuals search engine

38, 40, 42	5
48	6
46, 56	7

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
- DSCP priority values are mapped to default Class of Service values according to recommendations in the IEEE 802.1p standard, and then subsequently mapped to the eight hardware priority queues.
- This command sets the IP DSCP priority for all interfaces.

Example

The following example shows how to map IP DSCP value 1 to CoS value 0:

```
Console(config)#interface ethernet 1/5
Console(config-if)#map ip dscp 1 cos 0
Console(config-if)#
```

show map ip port

Use this command to show the IP port priority map.

Syntax

show map ip port [*interface*]

interface

- **ethernet** *unit/port*
  - *unit* - This is device 1.
  - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-6)

Downloaded from www.Manualslib.com manuals search engine

Default Setting

None

Command Mode

Privileged Exec

Example

The following shows that HTTP traffic has been mapped to CoS value 0:

```
Console#show map ip port
TCP port mapping status: disabled

 Port      Port no. COS
 --------- -------- ---
  Eth 1/ 5       80   0
Console#
```

Related Commands

map ip port (Global Configuration) (3-85)
map ip port (Interface Configuration) (3-87)

show map ip precedence

This command shows the IP precedence priority map.

Syntax

show map ip precedence [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - This is device 1.
  - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-6)

Default Setting

None

Downloaded from www.Manualslib.com manuals search engine

Command Mode

Privileged Exec

Example

```
Console#show map ip precedence ethernet 1/5
Precedence mapping status: disabled

 Port      Precedence COS
 --------- ---------- ---
  Eth 1/ 5          0   0
  Eth 1/ 5          1   1
  Eth 1/ 5          2   2
  Eth 1/ 5          3   3
  Eth 1/ 5          4   4
  Eth 1/ 5          5   5
  Eth 1/ 5          6   6
  Eth 1/ 5          7   7
Console#
```

Related Commands

map ip precedence (Global Configuration) (3-88)
map ip precedence (Interface Configuration) (3-88)

show map ip dscp

This command shows the IP DSCP priority map.

Syntax

show map ip dscp [*interface*]

interface

- **ethernet** *unit/port*
  - *unit* - This is device 1.
  - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-6)

Default Setting

None

Downloaded from www.Manualslib.com manuals search engine

Command Mode

Privileged Exec

Example

```
Console#show map ip dscp ethernet 1/1
DSCP mapping status: disabled

 Port      DSCP COS
 --------- ---- ---
  Eth 1/ 1    0   0
  Eth 1/ 1    1   0
  Eth 1/ 1    2   0
  Eth 1/ 1    3   0
.
.
.
  Eth 1/ 1   61   0
  Eth 1/ 1   62   0
  Eth 1/ 1   63   0
Console#
```

Related Commands

map ip dscp (Global Configuration) (3-89)
map ip dscp (Interface Configuration) (3-90)

Downloaded from www.Manualslib.com manuals search engine

Multicast Filtering Commands

This switch uses IGMP (Internet Group Management Protocol) to query for any attached hosts that want to receive a specific multicast service. It identifies the ports containing hosts requesting a service and sends data out to those ports only. It then propagates the service request up to any neighboring multicast switch/router to ensure that it will continue to receive the multicast service.

Note that IGMP query can be enabled globally at Layer 2, or enabled for specific VLAN interfaces at Layer 3. (Layer 2 query is disabled if Layer 3 query is enabled.)

Command Groups	Function	Page
IGMP Snooping	Configures multicast groups via IGMP snooping or static assignment, sets the IGMP version, displays current snooping and query settings, and displays the multicast service and group members	3-96
IGMP Query (Layer 2)	Configures IGMP query parameters for multicast filtering at Layer 2	3-100
Static Multicast Routing	Configures static multicast router ports	3-105
IGMP (Layer 3)	Configures the IGMP protocol used with multicast routing	3-107

Downloaded from www.Manualslib.com manuals search engine

IGMP Snooping Commands

Command	Function	Mode	Page
ip igmp snooping	Enables IGMP snooping	GC	3-96
ip igmp snooping vlan static	Adds an interface as a member of a multicast group	GC	3-96
ip igmp snooping version	Configures the IGMP version for snooping	GC	3-97
show ip igmp snooping	Shows the IGMP snooping and query configuration	PE	3-98
show mac-address-table multicast	Shows the IGMP snooping MAC multicast list	PE	3-99

ip igmp snooping

This command enables IGMP snooping on this switch. Use the **no** form to disable it.

Syntax

[**no**] **ip igmp snooping**

Default Setting

Enabled

Command Mode

Global Configuration

Example

The following example enables IGMP snooping.

```
Console(config)#ip igmp snooping
Console(config)#
```

ip igmp snooping vlan static

This command adds a port to a multicast group. Use the **no** form to remove the port.

Downloaded from www.Manualslib.com manuals search engine

Syntax

[**no**] **ip igmp snooping vlan** *vlan-id* **static** *ip-address interface*

- *vlan-id* - VLAN ID (Range: 1-4094)
- *ip-address* - IP address for multicast group
- *interface*
  - **ethernet** *unit/port*
    - *unit* - This is device 1.
    - *port* - Port number.
  - **port-channel** *channel-id* (Range: 1-6)

Default Setting

None

Command Mode

Global Configuration

Example

The following shows how to statically configure a multicast group on a port:

```
Console(config)#ip igmp snooping vlan 1 static 224.0.0.12 ethernet 1/5
Console(config)#
```

ip igmp snooping version

This command configures the IGMP snooping version. Use the **no** form to restore the default.

Syntax

ip igmp snooping version {**1** | **2**}
no ip igmp snooping version

- **1** - IGMP Version 1
- **2** - IGMP Version 2

Downloaded from www.Manualslib.com manuals search engine

Default Setting

IGMP Version 2

Command Mode

Global Configuration

Command Usage

- All systems on the subnet must support the same version. If there are legacy devices in your network that only support Version 1, you will also have to configure this switch to use Version 1.
- Some commands are only enabled for IGMPv2, including **ip igmp query-max-response-time** and **ip igmp query-timeout**.

Example

The following configures the switch to use IGMP Version 1:

```
Console(config)#ip igmp snooping version 1
Console(config)#
```

show ip igmp snooping

This command shows the IGMP snooping configuration.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

See "Configuring IGMP Snooping and Query Parameters" on page 3-193 for a description of the displayed items.

Downloaded from www.Manualslib.com manuals search engine

Example

The following shows the current IGMP snooping configuration:

```
Console#show ip igmp snooping
 Service status: Enabled
 Querier status: Enabled
 Query count: 2
 Query interval: 125 sec
 Query max response time: 10 sec
 Router port expire time: 300 sec
 IGMP snooping version: Version 2
Console#
```

show mac-address-table multicast

This command shows known multicast addresses.

Syntax

show mac-address-table multicast [**vlan** *vlan-id*] [**user** | **igmp-snooping**]

- *vlan-id* - VLAN ID (1 to 4094)
- **user** - Display only the user-configured multicast entries.
- **igmp-snooping** - Display only entries learned through IGMP snooping.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

Member types displayed include IGMP or USER, depending on selected options.

Downloaded from www.Manualslib.com manuals search engine

Example

The following shows the multicast entries learned through IGMP snooping for VLAN 1:

```
Console#show mac-address-table multicast vlan 1 igmp-snooping
 VLAN M'cast IP addr. Member ports Type
 ---- --------------- ------------ -------
    1       224.1.2.3      Eth1/11    IGMP
Console#
```

IGMP Query Commands (Layer 2)

Command	Function	Mode	Page
ip igmp snooping querier	Allows this device to act as the querier for IGMP snooping	GC	3-100
ip igmp snooping query-count	Configures the query count	GC	3-101
ip igmp snooping query-interval	Configures the query interval	GC	3-102
ip igmp snooping query-max-response-time	Configures the report delay	GC	3-102
ip igmp snooping router-port-expire-time	Configures the query timeout	GC	3-104

ip igmp snooping querier

This command enables the switch as an IGMP querier. Use the **no** form to disable it.

Syntax

[**no**] **ip igmp snooping querier**

Default Setting

Enabled

Command Mode

Global Configuration

Downloaded from www.Manualslib.com manuals search engine

Command Usage

If enabled, the switch will serve as querier if elected. The querier is responsible for asking hosts if they want to receive multicast traffic.

Example

```
Console(config)#ip igmp snooping querier
Console(config)#
```

ip igmp snooping query-count

This command configures the query count. Use the **no** form to restore the default.

Syntax

ip igmp snooping query-count *count*
no ip igmp snooping query-count

count - The maximum number of queries issued for which there has been no response before the switch takes action to drop a client from the multicast group. (Range: 2-10)

Default Setting

2 times

Command Mode

Global Configuration

Command Usage

The query count defines how long the querier waits for a response from a multicast client before taking action. If a querier has sent a number of queries defined by this command, but a client has not responded, a countdown timer is started using the time defined by **ip igmp snooping query-max- response-time**. If the countdown finishes, and the client still has not responded, then that client is considered to have left the multicast group.

Downloaded from www.Manualslib.com manuals search engine

Example

The following shows how to configure the query count to 10:

```
Console(config)#ip igmp snooping query-count 10
Console(config)#
```

Related Commands

ip igmp snooping query-max-response-time (3-102)

ip igmp snooping query-interval

This command configures the query interval. Use the **no** form to restore the default.

Syntax

ip igmp snooping query-interval *seconds*
no ip igmp snooping query-interval

seconds - The frequency at which the switch sends IGMP host-query messages. (Range: 60-125)

Default Setting

125 seconds

Command Mode

Global Configuration

Example

The following shows how to configure the query interval to 100 seconds:

```
Console(config)#ip igmp snooping query-interval 100
Console(config)#
```

ip igmp snooping query-max-response-time

This command configures the query report delay. Use the **no** form to restore the default.

Downloaded from www.Manualslib.com manuals search engine

Syntax

ip igmp snooping query-max-response-time *seconds*
no ip igmp snooping query-max-response-time

seconds - The report delay advertised in IGMP queries. (Range: 5-30)

Default Setting

10 seconds

Command Mode

Global Configuration

Command Usage

- The switch must be using IGMPv2 for this command to take effect.
- This command defines the time after a query, during which a response is expected from a multicast client. If a querier has sent a number of queries defined by the **ip igmp snooping query-count**, but a client has not responded, a countdown timer is started using an initial value set by this command. If the countdown finishes, and the client still has not responded, then that client is considered to have left the multicast group.

Example

The following shows how to configure the maximum response time to 20 seconds:

```
Console(config)#ip igmp snooping query-max-response-time 20
Console(config)#
```

Related Commands

ip igmp snooping version (3-97)
ip igmp snooping query-max-response-time (3-102)

Downloaded from www.Manualslib.com manuals search engine

ip igmp snooping router-port-expire-time

This command configures the query timeout. Use the **no** form to restore the default.

Syntax

ip igmp snooping router-port-expire-time *seconds*
no ip igmp snooping router-port-expire-time

seconds - The time the switch waits after the previous querier stops before it considers the router port (i.e., the interface which had been receiving query packets) to have expired.
(Range: 300-500)

Default Setting

300 seconds

Command Mode

Global Configuration

Command Usage

The switch must use IGMPv2 for this command to take effect.

Example

The following shows how to configure the default timeout to 300 seconds:

```
Console(config)#ip igmp snooping router-port-expire-time 300
Console(config)#
```

Related Commands

ip igmp snooping version (3-97)

Downloaded from www.Manualslib.com manuals search engine

Static Multicast Routing Commands

Command	Function	Mode	Page
ip igmp snooping vlan mrouter	Adds a multicast router port	GC	3-105
show ip igmp snooping mrouter	Shows multicast router ports	PE	3-106

ip igmp snooping vlan mrouter

This command statically configures a multicast router port. Use the **no** form to remove the configuration.

Syntax

[**no**] **ip igmp snooping vlan** *vlan-id* **mrouter** *interface*

- *vlan-id* - VLAN ID (Range: 1-4094)
- *interface*
  - **ethernet** *unit/port*
    - *unit* - This is device 1.
    - *port* - Port number.
  - **port-channel** *channel-id* (Range: 1-6)

Default Setting

No static multicast router ports are configured.

Command Mode

Global Configuration

Command Usage

Depending on your network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router/switch connected over the network to an interface (port or trunk) on your router, you can manually configure that interface to join all the current multicast groups.

Downloaded from www.Manualslib.com manuals search engine

Example

The following shows how to configure port 11 as a multicast router port within VLAN 1:

```
Console(config)#ip igmp snooping vlan 1 mrouter ethernet 1/11
Console(config)#
```

show ip igmp snooping mrouter

This command displays information on statically configured and dynamically learned multicast router ports.

Syntax

show ip igmp snooping mrouter [**vlan** *vlan-id*]

vlan-id - VLAN ID (Range: 1-4094)

Default Setting

Displays multicast router ports for all configured VLANs.

Command Mode

Privileged Exec

Command Usage

Multicast router port types displayed include Static or Dynamic.

Example

The following shows that port 11 in VLAN 1 is attached to a multicast router:

```
Console#show ip igmp snooping mrouter vlan 1
 VLAN M'cast Router Ports Type
 ---- ------------------- -------
    1            Eth 1/11  Static
    2            Eth 1/12  Dynamic
Console#
```


Downloaded from www.Manualslib.com manuals search engine

IGMP Commands (Layer 3)

Command	Function	Mode	Page
ip igmp	Enables IGMP for the specified interface	IC	3-107
ip igmp robustval	Configures the expected packet loss	IC	3-108
ip igmp query-interval	Configures frequency for sending host query messages	IC	3-109
ip igmp max-resp-interval	Configures the maximum host response time	IC	3-110
ip igmp last-memb-query-interval	Configures frequency for sending group-specific host query messages	IC	3-111
ip igmp version	Configures IGMP version used on this interface	IC	3-112
show ip igmp interface	Displays the IGMP configuration for specified interfaces	NE, PE	3-113
clear ip igmp group	Deletes entries from the IGMP cache	PE	3-113
show ip igmp groups	Displays detailed information for IGMP groups	NE, PE	3-114

ip igmp

Use this command to enable IGMP on a VLAN interface. Use the **no** form of this command to disable IGMP on the specified interface.

Syntax

ip igmp
no ip igmp

Default Setting

Disabled

Command Mode

Interface Configuration (VLAN)

Downloaded from www.Manualslib.com manuals search engine

Command Usage

IGMP query can be enabled globally at Layer 2 via the **ip igmp snooping** command, or enabled for specific VLAN interfaces at Layer 3 via the **ip igmp** command. (Layer 2 query is disabled if Layer 3 query is enabled.)

Example

```
Console(config)#interface vlan 1
Console(config-if)#ip igmp
Console(config-if)#end
Console#show ip igmp interface
Vlan 1 is up
  IGMP is enable, version is 2
  Robustness variable is 2
  Query interval is 125 sec
  Query Max Response Time is 10 sec, Last Member Query Interval is 1 sec
  Querier is 10.1.0.253

Console#
```

Related Commands

ip igmp snooping (3-96)
show ip igmp snooping (3-98)

ip igmp robustval

Use this command to specify the robustness (i.e., expected packet loss) for this interface. Use the **no** form of this command to restore the default value.

Syntax

ip igmp robustval *robust-value*
no ip igmp robustval

robust-value - The robustness of this interface. (Range: 1-255)

Default Setting

2

Downloaded from www.Manualslib.com manuals search engine

Command Mode

Interface Configuration (VLAN)

Command Usage

The robustness value is used in calculating the appropriate range for other IGMP variables, such as the Group Membership Interval (**ip igmp last-memb-query-interval**, page 3-111), as well as the Other Querier Present Interval, and the Startup Query Count (RFC 2236).

Example

```
Console(config-if)#ip igmp robustval 3
Console(config-if)#
```

ip igmp query-interval

Use this command to configure the frequency at which host query messages are sent. Use the **no** form to restore the default.

Syntax

ip igmp query-interval *seconds*
no ip igmp query-interval

seconds - The frequency at which the switch sends IGMP host-query messages. (Range: 1-255)

Default Setting

125 seconds

Command Mode

Interface Configuration (VLAN)

Command Usage

- Multicast routers send host query messages to determine the interfaces that are connected to downstream hosts requesting a specific multicast service. Only the designated multicast router for a subnet sends host query messages, which are addressed to the multicast address 224.0.0.1.
- For IGMP Version 1, the designated router is elected according to the

Downloaded from www.Manualslib.com manuals search engine

multicast routing protocol that runs on the LAN. But for IGMP Version 2, the designated querier is the lowest IP-addressed multicast router on the subnet.

Example

The following shows how to configure the query interval to 100 seconds:

```
Console(config-if)#ip igmp query-interval 100
Console(config-if)#
```

ip igmp max-resp-interval

Use this command to configure the maximum response time advertised in IGMP queries. Use the **no** form of this command to restore the default.

Syntax

ip igmp max-resp-interval *seconds*
no ip igmp max-resp-interval

seconds - The report delay advertised in IGMP queries. (Range: 1-255)

Default Setting

10 seconds

Command Mode

Interface Configuration (VLAN)

Command Usage

- The switch must be using IGMPv2 for this command to take effect.
- This command defines how long any responder (i.e., client or router) still in the group has to respond to a query message before the router deletes the group.
- By varying the Maximum Response Interval, you can tune the burstiness of IGMP messages passed on the subnet; where larger values make the traffic less bursty, as host responses are spread out over a larger interval.

Downloaded from www.Manualslib.com manuals search engine

- The number of seconds represented by the maximum response interval must be less than the Query Interval (page 3-109).

Example

The following shows how to configure the maximum response time to 20 seconds:

```
Console(config-if)#ip igmp max-resp-interval 20
Console(config-if)#
```

Related Commands

ip igmp version (3-112)
ip igmp query-interval (3-109)

ip igmp last-memb-query-interval

Use this command to configure the last member query interval. Use the **no** form of this command to restore the default.

Syntax

ip igmp last-memb-query-interval *seconds*
no ip igmp last-memb-query-interval

seconds - The report delay for the last member query. (Range: 1-255)

Default Setting

1 second

Command Mode

Interface Configuration (VLAN)

Command Usage

- A multicast client sends an IGMP leave message when it leaves a group. The router then checks to see if this was the last host in the group by sending an IGMP query and starting a timer based on this command. If no reports are received before the timer expires, the group is deleted.
- This value may be tuned to modify the leave latency of the network. A

Downloaded from www.Manualslib.com manuals search engine

reduced value results in reduced time to detect the loss of the last member of a group.

Example

The following shows how to configure the maximum response time to 10 seconds:

```
Console(config-if)#ip igmp last-memb-query-interval 10
Console(config-if)#
```

ip igmp version

Use this command to configure the IGMP version used on an interface. Use the **no** form of this command to restore the default.

Syntax

ip igmp version {**1** | **2**}
no ip igmp version

- **1** - IGMP Version 1
- **2** - IGMP Version 2

Default Setting

IGMP Version 2

Command Mode

Interface Configuration (VLAN)

Command Usage

- All routers on the subnet must support the same version. However, the multicast hosts on the subnet may support either IGMP version 1 or 2.
- The switch must be set to version 2 to enable the **ip igmp max-resp-interval** (page 3-110).

Downloaded from www.Manualslib.com manuals search engine

Example

The following configures the switch to use IGMP Version 1 on the selected interface:

```
Console(config-if)#ip igmp version 1
Console(config-if)#
```

show ip igmp interface

Use this command to show the IGMP configuration for a specific VLAN interface or for all interfaces.

Syntax

show ip igmp interface [**vlan** *vlan-id*]

vlan-id - VLAN ID (Range: 1-4094)

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Example

The following example shows the IGMP configuration for VLAN 1, as well as the device currently serving as the IGMP querier for this multicast service.

```
Console#show ip igmp interface vlan 1
Vlan 1 is up
  IGMP is enable, version is 2
  Robustness variable is 2
  Query interval is 125 sec
  Query Max Response Time is 10 sec, Last Member Query Interval is 1 sec
  Querier is 10.1.0.253
Console#
```

clear ip igmp group

Use this command to delete entries from the IGMP cache.

Downloaded from www.Manualslib.com manuals search engine

Syntax

clear ip igmp group [*group-address* | **interface vlan** *vlan-id*]

- *group-address* - IP address of the multicast group.
- *vlan-id* - VLAN ID (Range: 1-4094)

Default Setting

Deletes all entries in the cache if no options are selected.

Command Mode

Privileged Exec

Command Usage

Enter the address for a multicast group to delete all entries for the specified group. Enter the interface option to delete all multicast groups for the specified interface. Enter no options to clear all multicast groups from the cache.

Example

The following example clears all multicast group entries for VLAN 1:

```
Console#clear ip igmp group interface vlan 1
Console#
```

show ip igmp groups

Use this command to display information on multicast groups active on this switch.

Syntax

show ip igmp groups [*group-address* | **interface vlan** *vlan-id*]

- *group-address* - IP address of the multicast group.
- *vlan-id* - VLAN ID (Range: 1-4094)

Default Setting

Displays information for all known groups.

Downloaded from www.Manualslib.com manuals search engine

Command Mode

Normal Exec, Privileged Exec

Command Usage

- This command displays information for multicast groups learned via IGMP, not static groups.
- If the switch receives an IGMP Version 1 Membership Report, it sets a timer to note that there are Version 1 hosts present which are members of the group for which it heard the report.
- If there are Version 1 hosts present for a particular group, the switch will ignore any Leave Group messages that it receives for that group.

Example

The following shows the IGMP groups currently active on VLAN 1:

```
Console#show ip igmp groups vlan 1

 GroupAddress    InterfaceVlan   Lastreporter    Uptime   Expire   V1Timer
--------------- --------------- --------------- -------- -------- ---------
      234.5.6.8               1       10.1.5.19     7068      220         0
Console#
```

Field	Description
GroupAddress	IP multicast group address with subscribers directly attached or downstream from this switch.
InterfaceVlan	The interface on this switch that has received traffic directed to the multicast group address.
Lastreporter	The IP address of the source of the last membership report received for this multicast group address on this interface. If no membership report has been received, this object has the value 0.0.0.0.
Uptime	The time elapsed since this entry was created.
Expire	The time remaining before this entry will be aged out. (The default is 260 seconds.)
V1Timer	The time remaining until the switch assumes that there are no longer any IGMP Version 1 members on the IP subnet attached to this interface. (The default is 400 seconds.)

Downloaded from www.Manualslib.com manuals search engine

IP Interface Commands

There are no IP addresses assigned to this router by default. You must manually configure a new address to manage the router over your network or to connect the router to existing IP subnets. You may also need to a establish a default gateway between this device and management stations or other devices that exist on another network segment (if routing is not enabled).

This section includes commands for configuring IP interfaces, the Address Resolution Protocol (ARP) and Proxy ARP. These commands are used to connect subnetworks to the enterprise network.

Command Group	Function	Page
Basic IP Configuration	Configures the IP address for interfaces and the gateway router	3-116
Address Resolution Protocol (ARP)	Configures static, dynamic and proxy ARP service	3-122

Basic IP Configuration

Command	Function	Mode	Page
ip address	Sets the IP address for the current interface	IC	3-116
ip default-gateway	Defines the default gateway through which this router can reach other subnetworks	GC	3-118
show ip interface	Displays the IP settings for this device	PE	3-119
show ip redirects	Displays the default gateway configured for this device	PE	3-120
ping	Sends ICMP echo request packets to another node on the network	NE, PE	3-120

ip address

This command sets the IP address for the currently selected VLAN interface. Use the **no** form to restore the default IP address.

Downloaded from www.Manualslib.com manuals search engine

Syntax

ip address {*ip-address netmask* | **bootp** | **dhcp**} [*secondary*]
no ip address

- *ip-address* - IP address
- *netmask* - Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.
- **bootp** - Obtains IP address from BOOTP.
- **dhcp** - Obtains IP address from DHCP.
- *secondary* - Specifies a secondary IP address.

Default Setting

IP address: 0.0.0.0
Netmask: 255.0.0.0

Command Mode

Interface Configuration (VLAN)

Command Usage

- If this router is directly connected to end node devices (or connected to end nodes via shared media) that will be assigned to a specific subnet, then you must create a router interface for each VLAN that will support routing. The router interface consists of an IP address and subnet mask. This interface address defines both the network number to which the router interface is attached and the router's host number on that network. In other words, a router interface address defines the network and subnetwork numbers of the segment that is connected to that interface, and allows you to send IP packets to or from the router.
- Before you configure any network interfaces on this router, you should first create a VLAN for each unique user group, or for each network application and its associated users. Then assign the ports associated with each of these VLANs.
- You must assign an IP address to this device to gain management access over the network or to connect the router to existing IP subnets. You can manually configure a specific IP address, or direct the device to obtain an address from a BOOTP or DHCP server. Valid IP addresses consist of four numbers, 0 to 255, separated by periods.

Downloaded from www.Manualslib.com manuals search engine

Anything outside this format will not be accepted by the configuration program.

- An interface can have only one primary IP address, but can have many secondary IP addresses. In other words, you will need to specify secondary addresses if more than one IP subnet can be accessed via this interface.
- If you select the **bootp** or **dhcp** option, IP is enabled but will not function until a BOOTP or DHCP reply has been received. Requests will be broadcast periodically by this device in an effort to learn its IP address. (BOOTP and DHCP values can include the IP address, default gateway, and subnet mask).
- You can start broadcasting BOOTP or DHCP requests by entering an **ip dhcp restart client** command, or by rebooting the router.

Notes:1. Each VLAN group can be assigned its own IP interface address. Therefore, if routing is enabled, you can manage the router via any of these IP addresses.

2. Before you can change the primary IP address on an interface, you must first clear the current address with the no form of this command.

Example

In the following example, the device is assigned an address in VLAN 1.

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.5 255.255.255.0
Console(config-if)#
```

Related Commands

ip dhcp restart client (3-156)

ip default-gateway

This command establishes a static route between this router and devices that exist on another network segment. Use the **no** form to remove the static route.

Downloaded from www.Manualslib.com manuals search engine

Syntax

ip default-gateway *gateway*
no ip default-gateway

gateway - IP address of the default gateway

Default Setting

No static route is established.

Command Mode

Global Configuration

Command Usage

- The gateway specified in this command is only valid if routing is disabled with the **no ip routing** command. If IP routing is disabled, you must define a gateway if the target device is located in a different subnet.
- If routing is enabled, you must define the gateway with the **ip route** command.

Example

The following example defines a default gateway for this device:

```
Console(config)#ip default-gateway 10.1.1.254
Console(config)#
```

Related Commands

show ip redirects (3-120)
ip routing (3-127)
ip route (3-128)

show ip interface

This command displays the settings of an IP interface.

Default Setting

All interfaces

Command Mode

Privileged Exec

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console#show ip interface

Vlan 1 is up, addressing mode is User
  Interface address is 10.1.0.254, mask is 255.255.255.0, Primary
  MTU is 1500 bytes
  Proxy ARP is disabled
  Split horizon is enabled
Console#
```

Related Commands

show ip redirects (3-120)

show ip redirects

This command shows the default gateway configured for this device.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show ip redirects
ip default gateway 10.1.0.254
Console#
```

Related Commands

ip default-gateway (3-118)

ping

This command sends ICMP echo request packets to another node on the network.

Syntax

ping *host* [**count** *count*][**size** *size*]

- *host* - IP address or IP alias of the host.
- *count* - Number of packets to send. (Range: 1-16, default: 5)

Downloaded from www.Manualslib.com manuals search engine

- *size* - Number of bytes in a packet. (Range: 32-512, default: 32)
  The actual packet size will be eight bytes larger than the size specified because the router adds header information.

Default Setting

This command has no default for the host.

Command Mode

Normal Exec, Privileged Exec

Command Usage

- Use the ping command to see if another site on the network can be reached.
- Following are some results of the **ping** command:

- *Normal response* - The normal response occurs in one to ten seconds, depending on network traffic.
- *Destination does not respond* - If the host does not respond, a "timeout" appears in ten seconds.
- *Destination unreachable* - The gateway for this destination indicates that the destination is unreachable.
- *Network or host unreachable* - The gateway found no corresponding entry in the route table.

- Press <Esc> to stop pinging.

Example

```
Console#ping 10.1.0.9
Type ESC to abort.
PING to 10.1.0.9, by 5 32-byte payload ICMP packets, timeout is 5 seconds
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 0 ms
Ping statistics for 10.1.0.9:
 5 packets transmitted, 5 packets received (100%), 0 packets lost (0%)
Approximate round trip times:
 Minimum = 0 ms, Maximum = 10 ms, Average = 8 ms
Console#
```

Related Commands

interface (3-1)

Downloaded from www.Manualslib.com manuals search engine

Address Resolution Protocol (ARP)

Command	Function	Mode	Page
arp	Adds a static entry in the ARP cache	GC	3-122
arp-timeout	Sets the time a dynamic entry remains in the ARP cache	GC	3-123
clear arp-cache	Deletes all dynamic entries from the ARP cache	PE	3-124
show arp	Displays entries in the ARP cache	NE, PE	3-124
ip proxy-arp	Enables proxy ARP service	VC	3-125

arp

Use this command to add a static entry in the Address Resolution Protocol (ARP) cache. Use the **no** form to remove an entry from the cache.

Syntax

arp *ip-address hardware-address*
no arp *ip-address*

- *ip-address* - IP address to map to a specified hardware address.
- *hardware-address* - Hardware address to map to a specified IP address. (The format for this address is xx-xx-xx-xx-xx-xx.)

Default Setting

No default entries

Command Mode

Global Configuration

Command Usage

- The ARP cache is used to map 32-bit IP addresses into 48-bit hardware (i.e., Media Access Control) addresses. This cache includes entries for hosts and other routers on local network interfaces defined on this router.
- The maximum number of static entries allowed in the ARP cache is

Downloaded from www.Manualslib.com manuals search engine

128.

- You may need to enter a static entry in the cache if there is no response to an ARP broadcast message. For example, some applications may not respond to ARP requests or the response arrives too late, causing network operations to time out.

Example

```
Console(config)#arp 10.1.0.19 01-02-03-04-05-06
Console(config)#
```

Related Commands

clear arp-cache
show arp

arp-timeout

Use this command to set the aging time for dynamic entries in the Address Resolution Protocol (ARP) cache. Use the **no** form to restore the default.

Syntax

arp-timeout *seconds*
no arp-timeout

seconds - The time a dynamic entry remains in the ARP cache. (Range: 300-86400; 86400 is one day)

Default Setting

1200 seconds (20 minutes)

Command Mode

Global Configuration

Command Usage

Use the **show arp** command to display the current cache timeout value.

Example

This example sets the ARP cache timeout for 15 minutes (i.e., 900 seconds).

```
Console(config)#arp-timeout 900
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

clear arp-cache

Use this command to delete all dynamic entries from the Address Resolution Protocol (ARP) cache.

Command Mode

Privileged Exec

Example

This example clears all dynamic entries in the ARP cache.

```
Console#clear arp-cache
This operation will delete all the dynamic entries in ARP Cache.
Are you sure to continue this operation (y/n)?y
Console#
```

show arp

Use this command to display entries in the Address Resolution Protocol (ARP) cache.

Command Mode

Normal Exec, Privileged Exec

Command Usage

This command displays information about the ARP cache. The first line shows the cache timeout. It also shows each cache entry, including the corresponding IP address, MAC address, type (static, dynamic, other), and VLAN interface. Note that entry type "other" indicates local addresses for this router.

Downloaded from www.Manualslib.com manuals search engine

Example

This example displays all entries in the ARP cache.

```
Console#show arp
Arp cache timeout: 1200 (seconds)

    IP Address       MAC Address      Type   Interface
--------------- ----------------- --------- -----------
       10.1.0.0 ff-ff-ff-ff-ff-ff     other           1
     10.1.0.254 00-00-ab-cd-00-00     other           1
     10.1.0.255 ff-ff-ff-ff-ff-ff     other           1
  123.20.10.123 02-10-20-30-40-50    static           2
   345.30.20.23 09-50-40-30-20-10   dynamic           3

Total entry : 5
Console#
```

ip proxy-arp

Use this command to enable proxy Address Resolution Protocol (ARP). Use the **no** form to disable proxy ARP.

Syntax

ip proxy-arp
no ip proxy-arp

Default Setting

Disabled

Command Mode

Interface Configuration (VLAN)

Command Usage

Proxy ARP allows a non-routing device to determine the MAC address of a host on another subnet or network.

Example

```
Console(config)#interface vlan 3
Console(config-if)#ip proxy-arp
Console(config-if)#
```


Downloaded from www.Manualslib.com manuals search engine

IP Routing Commands

After you configure network interfaces for this router, you must set the paths used to send traffic between different interfaces. If you enable routing on this device, traffic will automatically be forwarded between all of the local subnetworks. However, to forward traffic to devices on other subnetworks, you can either configure fixed paths with static routing commands, or enable a dynamic routing protocol that exchanges information with other routers on the network to automatically determine the best path to any subnetwork.

This section includes commands for both static and dynamic routing. These commands are used to connect between different local subnetworks or to connect the router to the enterprise network.

Command Group	Function	Page
Global Routing Configuration	Configures global parameters for static and dynamic routing, displays the routing table, and statistics for protocols used to exchange routing information	3-127
Routing Information Protocol (RIP)	Configures global and interface specific parameters for RIP	3-131
Open Shortest Path First (OSPF)	Configures global and interface specific parameters for OSPF	3-144

Downloaded from www.Manualslib.com manuals search engine

Global Routing Configuration

Command	Function	Mode	Page
ip routing	Enables static and dynamic IP routing	GC	3-127
ip route	Configures static routes	GC	3-128
clear ip route	Deletes specified entries from the routing table	PE	3-129
show ip route	Displays specified entries in the routing table	PE	3-129
show ip traffic	Displays statistics for IP, ICMP, UDP, TCP and ARP protocols	PE	3-130

ip routing

Use this command to enable IP routing. Use the **no** form to disable IP routing.

Syntax

ip routing
no ip routing

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

- The command affects both static and dynamic unicast routing.
- If IP routing is enabled, all IP packets are routed using either static routing or dynamic routing via RIP or OSPF, and other packets for all non-IP protocols (e.g., NetBuei, NetWare or AppleTalk) are switched based on MAC addresses. If IP routing is disabled, all packets are switched, with filtering and forwarding decisions based strictly on MAC addresses.

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console(config)#ip routing
Console(config)#
```

ip route

Use this command to configure static routes. Use the **no** form to remove static routes.

Syntax

ip route {*destination-ip netmask* | **default**} {*gateway*} [**metric** *metric*]
no ip route {*destination-ip netmask* | **default** | *****}

- *destination-ip* – IP address of the destination network, subnetwork, or host.
- *netmask* - Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.
- **default** – Sets this entry as the default route.
- *gateway* – IP address of the gateway used for this route.
- *metric* – Selected RIP cost for this interface. (Range: 1-5, default: 1)
- ***** – Removes all static routing table entries.

Default Setting

No static routes are configured.

Command Mode

Global Configuration

Command Usage

- You can configure up to 2000 static routes.
- Static routes take precedence over dynamically learned routes.
- Static routes are included in RIP updates periodically sent by the router.

Example

This example forwards all traffic for subnet 192.168.1.0 to the router 192.168.5.254, using the default metric of 1.

```
Console(config)#ip route 192.168.1.0 255.255.255.0 192.168.5.254
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

clear ip route

Use this command to remove dynamically learned entries from the IP routing table.

Syntax

clear ip route {*network* [*netmask*] | *****}

- *network* – Network or subnet address.
- *netmask* - Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.
- ***** – Removes all dynamic routing table entries.

Command Mode

Privileged Exec

Command Usage

- This command only clears dynamically learned routes.
- Use the **no ip address** command to remove a local interface.
- Use the **no ip route** command to remove a static route.

Example

```
Console#clear ip route 10.1.5.0
Console#
```

show ip route

Use this command to display information in the IP routing table.

Syntax

show ip route [**config** | *address* [*netmask*]]

- **config** – Displays all static routing entries.
- *address* – IP address of the destination network, subnetwork or host for which routing information is to be displayed.
- *netmask* - Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.

Command Mode

Privileged Exec

Downloaded from www.Manualslib.com manuals search engine

Command Usage

If the *address* is specified without the *netmask* parameter, the router displays all routes for the corresponding natural class address (page 3-134).

Example

```
Console#show ip route

  Ip Address        Netmask        Next Hop      Protocol  Metric Interface
--------------- --------------- --------------- ---------- ------ ---------
        0.0.0.0         0.0.0.0     10.2.48.102     static      0         1
      10.2.48.2   255.255.252.0      10.2.48.16      local      0         1
       10.2.5.6   255.255.255.0       10.2.8.12        RIP      1         2
       10.3.9.1   255.255.255.0      10.2.9.254 OSPF-intra      2         3


Total entry: 4
Console#
```

Field	Description
Ip Address	IP address of the destination network, subnetwork, or host. Note that the address 0.0.0.0 indicates the default gateway for this router.
Netmask	Network mask for the associated IP subnet.
Next Hop	IP address of the next hop (or gateway) used for this route.
Protocol	The protocol which generated this route information. (Values: static, local, RIP, OSPF)
Metric	Cost for this interface.
Interface	VLAN interface through which this address can be reached.

show ip traffic

Use this command to display statistics for IP, ICMP, UDP, TCP and ARP protocols.

Command Mode

Privileged Exec

Command Usage

For a description of the information shown by this command, see "Displaying Statistics for IP Protocols" on page 3-263.

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console#show ip traffic
IP statistics:
  Rcvd:  5 total, 5 local destination
         0 checksum errors
         0 unknown protocol, 0 not a gateway
  Frags: 0 reassembled, 0 timeouts
         0 fragmented, 0 couldn't fragment
  Sent:  9 generated
         0 no route
ICMP statistics:
  Rcvd: 0 checksum errors, 0 redirects, 0 unreachable, 0 echo
        5 echo reply, 0 mask requests, 0 mask replies, 0 quench
        0 parameter, 0 timestamp
  Sent: 0 redirects, 0 unreachable, 0 echo, 0 echo reply
        0 mask requests, 0 mask replies, 0 quench, 0 timestamp
        0 time exceeded, 0 parameter problem
UDP statistics:
  Rcvd: 0 total, 0 checksum errors, 0 no port
  Sent: 0 total
TCP statistics:
  Rcvd: 0 total, 0 checksum errors
  Sent: 0 total
ARP statistics:
  Rcvd: 0 requests, 1 replies
  Sent: 1 requests, 0 replies
Console#
```

Routing Information Protocol (RIP)

Command	Function	Mode	Page
router rip	Enables the RIP routing protocol	GC	3-132
timers basic	Sets basic timers, including update, timeout, garbage collection	RC	3-133
network	Specifies the network interfaces that are to use RIP routing	RC	3-134
neighbor	Defines a neighboring router with which to exchange information	RC	3-135
version	Specifies the RIP version to use on all network interfaces (if not already specified with a receive version or send version command)	RC	3-135
ip rip receive version	Sets the RIP receive version to use on a network interface	IC	3-137

Downloaded from www.Manualslib.com manuals search engine

Command	Function	Mode	Page
ip rip send version	Sets the RIP send version to use on a network interface	IC	3-138
ip split-horizon	Enables split-horizon or poison-reverse loop prevention	IC	3-139
ip rip authentication key	Enables authentication for RIP2 packets and specifies keys	IC	3-140
ip rip authentication mode	Specifies the type of authentication used for RIP2 packets	IC	3-141
show rip globals	Displays global configuration settings and statistics for RIP	PE	3-142
show ip rip	Displays RIP configuration information for each network interface	PE	3-143

router rip

Use this command to enable Routing Information Protocol (RIP) routing for all IP interfaces on the router. Use the **no** form to disable it.

Syntax

router rip
no router rip

Command Mode

Global Configuration

Default Setting

Disabled

Command Usage

- RIP is used to specify how routers exchange routing table information.
- This command is also used to enter router configuration mode.

Example

```
Console(config)#router rip
Console(config-router)#
```


Downloaded from www.Manualslib.com manuals search engine

Related Commands

network (3-134)

timers basic

Use this command to configure the RIP update timer, timeout timer, and garbage- collection timer. Use the **no** form to restore the defaults.

Syntax

timers basic *update-seconds*
no timers basic

update-seconds – Sets the update timer to the specified value, sets the timeout time value to 6 times the update time, and sets the garbage-collection timer to 4 times the update time.
(Range for update timer: 15-60 seconds)

Command Mode

Router Configuration

Default Setting

Update: 30 seconds
Timeout: 180 seconds
Garbage collection: 120 seconds

Command Usage

- The *update* timer sets the rate at which updates are sent. This is the fundamental timer used to control all basic RIP processes.
- The *timeout* timer is the time after which there have been no update messages that a route is declared dead. The route is marked inaccessible (i.e., the metric set to infinite) and advertised as unreachable. However, packets are still forwarded on this route.
- After the *timeout* interval expires, the router waits for an interval specified by the *garbage-collection* timer before removing this entry from the routing table. This timer allows neighbors to become aware of an invalid route prior to purging it.
- Setting the update timer to a short interval can cause the router to spend an excessive amount of time processing updates.
- These timers must be set to the same values for all routers in the

Downloaded from www.Manualslib.com manuals search engine

network.

Example

This example sets the update timer to 40 seconds. The timeout timer is subsequently set to 240 seconds, and the garbage-collection timer to 160 seconds.

```
Console(config-router)#timers basic 15
Console(config-router)#
```

network

Use this command to specify the network interfaces that will be included in the RIP routing process. Use the **no** form to remove an entry.

Syntax

network *subnet-address*
no network *subnet-address*

subnet-address – IP address of a network directly connected to this router.

Command Mode

Router Configuration

Default Setting

No networks are specified.

Command Usage

- RIP only sends updates to interfaces specified by this command.
- Subnet addresses are interpreted as class A, B or C, based on the first field in the specified address. In other words, if a subnet address nnn.xxx.xxx.xxx is entered, the first field (nnn) determines the class:

  0 - 127 is class A, and only the first field in the network address is used.
  128 - 19 is class B, and the first two fields in the network address are used.
  192 - 223 is class C, and the first three fields in the network address are used.

Downloaded from www.Manualslib.com manuals search engine

Example

This example includes network interface 10.1.0.0 in the RIP routing process.

```
Console(config-router)#network 10.1.0.0
Console(config-router)#
```

Related Commands

router rip (3-132)

neighbor

Use this command to define a neighboring router with which this router will exchange routing information. Use the **no** form to remove an entry.

Syntax

neighbor *ip-address*
no neighbor *ip-address*

ip-address - IP address to map to a specified hardware address.

Command Mode

Router Configuration

Default Setting

No neighbors are defined.

Command Usage

This command can be used to configure a static neighbor with which this router will exchange information, rather than relying on broadcast messages generated by the RIP protocol.

Example

```
Console(config-router)#neighbor 10.2.0.254
Console(config-router)#
```

version

Use this command to specify a RIP version used globally by the router. Use the **no** form to restore the default value.

Downloaded from www.Manualslib.com manuals search engine

Syntax

version {**1** | **2**}
no version

- **1** - RIP Version 1
- **2** - RIP Version 2

Command Mode

Router Configuration

Default Setting

RIP Version 1

Command Usage

- When this command is used to specify a global RIP version, any VLAN interface not previously set by the **ip rip receive version** or **ip rip send version** command will be set to the following values:
  - RIP Version 1 configures the unset interfaces to send RIPv1 compatible protocol messages and receive either RIPv1 or RIPv2 protocol messages.
  - RIP Version 2 configures the unset interfaces to use RIPv2 for both sending and receiving protocol messages.
- When the **no** form of this command is used to restore the default value, any VLAN interface not previously set by the **ip rip receive version** or **ip rip send version** command will be set to the default send or receive version.

Example

This example sets the global version for RIP to send and receive version 2 packets.

```
Console(config-router)#version 2
Console(config-router)#
```

Related Commands

ip rip receive version (3-137)
ip rip send version (3-138)

Downloaded from www.Manualslib.com manuals search engine

ip rip receive version

Use this command to specify a RIP version to receive on an interface. Use the **no** form to restore the default value.

Syntax

ip rip receive version {**none** | **1** | **2** | **1 2**}
no ip rip receive version

- **none** - Does not accept incoming RIP packets.
- **1** - Accepts only RIPv1 packets.
- **2** - Accepts only RIPv2 packets.
- **1 2** - Accepts RIPv1 or RIPv2 packets

Command Mode

Interface Configuration (VLAN)

Default Setting

The default depends on the setting specified with the **version** command:

Global RIPv1 - RIPv1 or RIPv2 packets
Global RIPv2 - RIPv2 packets

Command Usage

- Use this command to override the global setting specified by the RIP **version** command.
- You can specify the receive version based on these options:
  - Use "none" if you do not want to add any dynamic entries to the routing table for an interface. (For example, you may only want to allow static routes for a specific interface.)
  - Use "1" or "2" if all routers in the local network are based on RIPv1 or RIPv2, respectively.
  - Use "1 2" if some routers in the local network are using RIPv2, but there are still some older routers using RIPv1.

Downloaded from www.Manualslib.com manuals search engine

Example

This example sets the interface version for VLAN 1 to receive RIPv1 packets.

```
Console(config)#interface vlan 1
Console(config-if)#ip rip receive version 1
Console(config-if)#
```

Related Commands

version (3-135)

ip rip send version

Use this command to specify a RIP version to send on an interface. Use the **no** form to restore the default value.

Syntax

ip rip send version {**none** | **1** | **2** | **v2-broadcast**}
no ip rip send version

- **none** - Does not transmit RIP updates.
- **1** - Sends only RIPv1 packets.
- **2** - Sends only RIPv2 packets.
- **v2-broadcast** - Route information is broadcast to other routers with RIPv2.

Command Mode

Interface Configuration (VLAN)

Default Setting

The default depends on the setting specified with the **version** command:

Global RIPv1 - Route information is broadcast to other routers with RIPv2

Global RIPv2 - RIPv2 packets

Command Usage

- Use this command to override the global setting specified by the RIP **version** command.
- You can specify the receive version based on these options:

Downloaded from www.Manualslib.com manuals search engine

- Use "none" to passively monitor route information advertised by other routers attached to the network.
- Use "1" or "2" if all routers in the local network are based on RIPv1 or RIPv2, respectively.
- Use "v2-broadcast" to propagate route information by broadcasting to other routers on the network using RIPv2, instead of multicasting as normally required by RIPv2. (Using this mode allows RIPv1 routers to receive these protocol messages, but still allows RIPv2 routers to receive the additional information provided by RIPv2, including subnet mask, next hop and authentication information.)

Example

This example sets the interface version for VLAN 1 to send RIPv1 packets.

```
Console(config)#interface vlan 1
Console(config-if)#ip rip send version 1
Console(config-if)#
```

Related Commands

version (3-135)

ip split-horizon

Use this command to enable split-horizon or poison-reverse (a variation) on an interface. Use the **no** form to disable split-horizon.

Syntax

ip split-horizon [**poison-reverse**]
no ip split-horizon

poison-reverse - Enables poison-reverse on the current interface.

Command Mode

Interface Configuration (VLAN)

Default Setting

split-horizon

Downloaded from www.Manualslib.com manuals search engine

Command Usage

- Split horizon never propagates routes back to an interface from which they have been acquired.
- Poison reverse propagates routes back to an interface port from which they have been acquired, but sets the distance-vector metrics to infinity. (This provides faster convergence.)

Example

This example propagates routes back to the source using poison-reverse.

```
Console(config)#interface vlan 1
Console(config-if)#ip split-horizon poison-reverse
Console(config-if)#
```

ip rip authentication key

Use this command to enable authentication for RIPv2 packets and to specify the key that must be used on an interface. Use the **no** form to prevent authentication.

Syntax

ip rip authentication key *key-string*
no ip rip authentication

key-string - A password used for authentication.
(Range: 1-16 characters, case sensitive)

Command Mode

Interface Configuration (VLAN)

Default Setting

No authentication

Command Usage

- This command can be used to restrict the interfaces that can exchange RIPv2 routing information. (Note that this command does not apply to RIPv1.)
- For authentication to function properly, both the sending and receiving interface must be configured with the same password.

Downloaded from www.Manualslib.com manuals search engine

Example

This example sets an authentication password of "small" to verify incoming routing messages and to tag outgoing routing messages.

```
Console(config)#interface vlan 1
Console(config-if)#ip rip authentication key small
Console(config-if)#
```

Related Commands

ip rip authentication mode (3-141)

ip rip authentication mode

Use this command to specify the type of authentication that can be used on an interface. Note that the current firmware version only supports a simple password. Use the **no** form to restore the default value.

Syntax

ip rip authentication mode {**text**}
no ip rip authentication mode

text - Indicates that a simple password will be used.

Command Mode

Interface Configuration (VLAN)

Default Setting

No authentication

Command Usage

- The password to be used for authentication is specified in the **ip rip authentication key** command (page 3-140).
- This command requires the interface to exchange routing information with other routers based on an authorized password. (Note that this command only applies to RIPv2.)
- For authentication to function properly, both the sending and receiving interface must be configured with the same password or authentication key.

Downloaded from www.Manualslib.com manuals search engine

Example

This example sets the authentication mode to plain text.

```
Console(config)#interface vlan 1
Console(config-if)#ip rip authentication mode text
Console(config-if)#
```

Related Commands

ip rip authentication key (3-140)

show rip globals

Use this command to display global configuration settings for RIP.

Command Mode

Privileged Exec

Example

```
Console#show rip globals

RIP Process: Enabled
Update Time in Seconds: 30
Number of Route Change: 0
Number of Queries: 1
Console#
```

Field	Description
RIP Process	Indicates if RIP has been enabled or disabled.
Update Time in Seconds	The interval at which RIP advertises known route information. (Default: 30 seconds)
Number of Route Changes	Number of times routing information has changed.
Number of Queries	Number of router database queries received by this router.

Downloaded from www.Manualslib.com manuals search engine

show ip rip

Use this command to display information about interfaces configured for RIP.

Syntax

show ip rip {**configuration** | **status** | **peer**}

- **configuration** - Shows RIP configuration settings for each interface.
- **status** - Shows the status of routing messages on each interface.
- **peer** - Shows information on neighboring routers, along with information about the last time a route update was received, the RIP version used by the neighbor, and the status of routing messages received from this neighbor.

Command Mode

Privileged Exec

Example

```
Console#show ip rip configuration

     Interface      SendMode      ReceiveMode     Poison       Authentication
--------------- --------------- ------------- --------------
------------------
    10.1.0.253  rip1Compatible    RIPv1Orv2  SplitHorizon  noAuthentication
    10.1.1.253  rip1Compatible    RIPv1Orv2  SplitHorizon  noAuthentication
Console#show ip rip status

     Interface   RcvBadPackets   RcvBadRoutes     SendUpdates
--------------- --------------- -------------- ---------------
     10.1.0.253               0              0              13
     10.1.1.253               0              0              13
Console#show ip rip peer

          Peer   UpdateTime   Version   RcvBadPackets   RcvBadRoutes
--------------- ------------ --------- --------------- --------------
     10.1.0.254         1625         2               0              0
     10.1.1.254         1625         2               0              0
Console#
```

Field	Description
show ip rip configuration	
Interface	IP address of the interface.

Downloaded from www.Manualslib.com manuals search engine

Field	Description
SendMode	RIP version sent on this interface (none, RIPv1, RIPv2, or RIPv2-broadcast)
ReceiveMode	RIP version received on this interface (none, RIPv1, RIPv2, RIPv1 or RIPv2)
Poison	Shows if split-horizon, poison-reverse, or no protocol message loopback prevention method is in use.
Authentication	Shows if authentication is set to simple password or none.
show ip rip status	
Interface	IP address of the interface.
RcvBadPackets	Number of bad RIP packets received.
RcvBadRoutes	Number of bad routes received.
SendUpdates	Number of route changes.
show ip rip peer	
Peer	IP address of a neighboring RIP router.
UpdateTime	Last time a route update was received from this peer.
Version	Whether RIPv1 or RIPv2 packets were received from this peer.
RcvBadPackets	Number of bad RIP packets received from this peer.
RcvBadRoutes	Number of bad routes received from this peer.

Open Shortest Path First (OSPF)

Command	Function	Mode	Page
General Configuration			
router ospf	Enables or disables OSPF	GC	3-146
router-id	Sets the router ID for this device	RC	3-147
compatible rfc1583	Calculates summary route costs using RFC 1583 (OSPFv1)	RC	3-148
default-information originate	Generates a default external route into an autonomous system	RC	3-149
timers spf	Configures the hold time between consecutive SPF calculations	RC	3-150

Downloaded from www.Manualslib.com manuals search engine

Command	Function	Mode	Page
Route Metrics and Summaries			
area range	Summarizes routes advertised by an ABR	RC	3-151
area default-cost	Sets the cost for a default summary route sent into a stub or NSSA	RC	3-152
summary-address	Summarizes routes advertised by an ASBR	RC	3-153
redistribute	Redistribute routes from one routing domain to another	RC	3-154
Area Configuration			
network area	Assigns specified interface to an area	RC	3-155
area stub	Defines a stubby area that cannot send or receive LSAs	RC	3-156
area nssa	Defines a not-so-stubby that can import external routes	RC	3-158
area virtual-link	Defines a virtual link from an area border routers to the backbone	RC	3-160
Interface Configuration			
ip ospf authentication	Specifies the authentication type for an interface	IC	3-163
ip ospf authentication-key	Assigns a simple password to be used by neighboring routers	IC	3-164
ip ospf message-digest-key	Enables MD5 authentication and sets the key for an interface	IC	3-165
ip ospf cost	Specifies the cost of sending a packet on an interface	IC	3-166
ip ospf dead-interval	Sets the interval at which hello packets are not seen before neighbors declare the router down	IC	3-166
ip ospf hello-interval	Specifies the interval between sending hello packets	IC	3-167
ip ospf priority	Sets the router priority used to determine the designated router	IC	3-168

Downloaded from www.Manualslib.com manuals search engine

Command	Function	Mode	Page
ip ospf retransmit-interval	Specifies the time between resending a link-state advertisement	IC	3-169
ip ospf transmit-delay	Estimates time to send a link-state update packet over an interface	IC	3-169
Display Information			
show ip ospf	Displays general information about the routing processes	PE	3-170
show ip ospf border-routers	Displays routing table entries for Area Border Routers (ABR) and Autonomous System Boundary Routers (ASBR)	PE	3-171
show ip ospf database	Shows information about different LSAs in the database	PE	3-172
show ip ospf interface	Displays interface information	PE	3-181
show ip ospf neighbor	Displays neighbor information	PE	3-182
show ip ospf summary-address	Displays all summary address redistribution information	PE	3-183
show ip ospf virtual-links	Displays parameters and the adjacency state of virtual links	PE	3-184

router ospf

Use this command to enable Open Shortest Path First (OSPF) routing for all IP interfaces on the router. Use the **no** form to disable it.

Syntax

router ospf
no router ospf

Command Mode

Global Configuration

Default Setting

Disabled

Downloaded from www.Manualslib.com manuals search engine

Command Usage

- OSPF is used to specify how routers exchange routing table information.
- This command is also used to enter router configuration mode.

Example

```
Console(config)#router ospf
Console(config-router)#
```

Related Commands

network area (3-155)

router-id

Use this command to assign a unique router ID for this device within the autonomous system. Use the **no** form to use the default router identification method (i.e., the lowest interface address).

Syntax

router-id *ip-address*
no router-id

ip-address - Router ID formatted as an IP address.

Command Mode

Router Configuration

Default Setting

Lowest interface address

Command Usage

- The router ID must be unique for every router in the autonomous system. Using the default setting based on the lowest interface address ensures that each router ID is unique. Also, note that you cannot set the router ID to 0.0.0.0 or 255.255.255.255.
- If this router already has registered neighbors, the new router ID will be used when the router is rebooted, or manually restarted by entering the **no router ospf** followed by the **router ospf** command.

Downloaded from www.Manualslib.com manuals search engine

- If the priority values of the routers bidding to be the designated router or backup designated router for an area are equal, the router with the highest ID is elected.

Example

```
Console(config-router)#router-id 10.1.1.1
Console(config-router)#
```

Related Commands

router ospf (3-146)

compatible rfc1583

Use this command to calculate summary route costs using RFC 1583 (OSPFv1). Use the **no** form to calculate costs using RFC 2328 (OSPFv2).

Syntax

compatible rfc1583
no compatible rfc1583

Command Mode

Router Configuration

Default Setting

RFC 1583 compatible

Command Usage

All routers in an OSPF routing domain should use the same RFC for calculating summary routes.

Example

```
Console(config-router)#compatible rfc1583
Console(config-router)#
```


Downloaded from www.Manualslib.com manuals search engine

default-information originate

Use this command to generate a default external route into an autonomous system. Use the **no** form to disable this feature.

Syntax

default-information originate [**always**] [**metric** *interface-metric*] [**metric-type** *metric-type*]

no default-information originate

- **always** - Always advertise a default route to the local AS regardless of whether the router has a default route. (See "ip route" on page 3-128.)
- *interface-metric* - Metric assigned to the default route. (Range: 1-65535; Default: 10)
- *metric-type* - External link type used to advertise the default route. (Options: Type 1, Type 2; Default: Type 2)

Command Mode

Router Configuration

Default Setting

Disabled

Command Usage

- The metric for the default external route is used to calculate the path cost for traffic passed from other routers within the AS out through the ASBR.
- When you use this command to redistribute routes into a routing domain (i.e., an Autonomous System, this router automatically becomes an Autonomous System Boundary Router (ASBR). However, an ASBR does not, by default, generate a default route into the routing domain.
  - If you use the **always** keyword, the router will advertise itself as a default external route into the AS, even if a default external route does not actually exist. (To define a default route, use the **ip route** command.)
  - If you do *not* use the **always** keyword, the router can only advertise a default external route into the AS if the **redistribute** command is

Downloaded from www.Manualslib.com manuals search engine

used to import external routes via RIP or static routing, and such a route is known.

- Type 1 route advertisements add the internal cost to the external route metric. Type 2 routes do not add the internal cost metric. When comparing Type 2 routes, the internal cost is only used as a tie-breaker if several Type 2 routes have the same cost.

Example

This example assigns a metric of 20 to the default external route advertised into an autonomous system, sending it as a Type 2 external metric.

```
Console(config-router)#default-information originate metric 20 metric-type
2
Console(config-router)#
```

Related Commands

ip route (3-128)
redistribute (3-154)

timers spf

Use this command to configure the hold time between making two consecutive shortest path first (SPF) calculations. Use the **no** form to restore the default value.

Syntax

timers spf *spf-holdtime*
no timers spf

spf-holdtime - Minimum time between two consecutive SPF calculations. (Range: 0-65535 seconds)

Command Mode

Router Configuration

Default Setting

10 seconds

Command Usage

- Setting the SPF holdtime to 0 means that there is no delay between consecutive calculations.

Downloaded from www.Manualslib.com manuals search engine

- Using a low value allows the router to switch to a new path faster, but uses more CPU processing time.

Example

```
Console(config-router)#timers spf 20
Console(config-router)#
```

area range

Use this command to summarize the routes advertised by an Area Border Router (ABR). Use the **no** form to disable this function.

Syntax

area *area-id* range *ip-address netmask* [advertise | not-advertise]
no area *area-id* **range** *ip-address netmask* [**advertise** | **not-advertise**]

- *area-id* - Identifies an area for which the routes are summarized. (The area ID must be in the form of an IP address.)
- *ip-address* - Base address for the routes to summarize.
- *netmask* - Network mask for the summary route.
- **advertise** - Advertises the specified address range.
- **not-advertise** - The summary is not sent, and the routes remain hidden from the rest of the network.

Command Mode

Router Configuration

Default Setting

Disabled

Command Usage

- This command can be used to advertise routes between areas.
- If routes are set to be advertised, the router will issue a Type 3 summary LSA for each address range specified with this command.
- This router supports up 64 summary routes for area ranges.

Downloaded from www.Manualslib.com manuals search engine

Example

This example creates a summary address for all area routes in the range of 10.2.x.x.

```
Console(config-router)#area 10.2.0.0 range 10.2.0.0 255.255.0.0 advertise
Console(config-router)#
```

area default-cost

Use this command to specify a cost for the default summary route sent into a stub or not-so-stubby area (NSSA) from an Area Border Router (ABR). Use the **no** form to remove the assigned default cost.

Syntax

area *area-id* **default-cost** *cost*
no area *area-id* **default-cost**

- *area-id* - Identifier for a stub or NSSA, in the form of an IP address.
- *cost* - Cost for the default summary route sent to a stub or NSSA. (Range: 0-65535)

Command Mode

Router Configuration

Default Setting

1

Command Usage

- If you enter this command for a normal area, it will changed to a stub.
- If the default cost is set to "0," the router will not advertise a default route into the attached stub or NSSA.

Example

```
Console(config-router)#area 10.3.9.0 default-cost 10
Console(config-router)#
```

Related Commands

area stub (3-156)

Downloaded from www.Manualslib.com manuals search engine

summary-address

Use this command to aggregate routes learned from other protocols. Use the **no** form to remove a summary address.

Syntax

summary-address *summary-address netmask*
no summary-address *summary-address netmask*

- *summary-address* - Summary address covering a range of addresses.
- *netmask* - Network mask for the summary route.

Command Mode

Router Configuration

Default Setting

Disabled

Command Usage

- An Autonomous System Boundary Router (ASBR) can redistribute routes learned from other protocols by advertising an aggregate route into all attached autonomous systems.
- This router supports up 16 Type-5 summary routes.

Example

This example creates a summary address for all routes contained in 192.168.x.x.

```
Console(config-router)#summary-address 192.168.0.0 255.255.0.0
Console(config-router)#
```

Related Commands

area range (3-151)

Downloaded from www.Manualslib.com manuals search engine

redistribute

Use this command to import external routing information from other routing domains (i.e., protocols) into the autonomous system. Use the **no** form to disable this feature.

Syntax

redistribute [**rip** | **static**] [**metric** *metric-value*] [**metric-type** *type-value*]
no redistribute [**rip** | **static**] [**metric** *metric-value*] [**metric-type** *type-value*]

- **rip** - External routes will be imported from the Routing Information Protocol into this Autonomous System.
- **static** - Static routes will be imported into this Autonomous System.
- *metric-value* - Metric assigned to all external routes for the specified protocol. (Range: 1-65535: Default: 10)
- *type-value*
  - **1** - Type 1 external route
  - **2** - Type 2 external route (default) - Routers do not add internal route metric to external route metric.

Command Mode

Router Configuration

Default Setting

redistribution - none
protocol - RIP and static
metric-value - 0
type-metric - 2

Command Usage

- This router supports redistribution for both RIP and static routes.
- When you redistribute external routes into an OSPF autonomous system (AS), the router automatically becomes an autonomous system boundary router (ASBR). If the **redistribute** command is used in conjunction with the **default-information originate** command to generate a "default" external route into the AS, the metric value specified in this command supersedes the metric specified in the **default-information originate** command.

Downloaded from www.Manualslib.com manuals search engine

- Metric type specifies the way to advertise routes to destinations outside the AS via External LSAs. Specify Type 1 to add the internal cost metric to the external route metric. In other words, the cost of the route from any router within the AS is equal to the cost associated with reaching the advertising ASBR, plus the cost of the external route. Specify Type 2 to only advertise the external route metric.

Example

This example redistributes routes learned from RIP as Type 1 external routes.

```
Console(config-router)#redistribute rip metric-type 1
Console(config-router)#
```

Related Commands

default-information originate (3-149)

network area

Use this command to define an OSPF area and the interfaces that operate within this area. Use the **no** form to disable OSPF for a specified interface.

Syntax

network *ip-address netmask* **area** *area-id*
no network *ip-address netmask* **area** *area-id*

- *ip-address* - Address of the interfaces to add to the area.
- *netmask* - Network mask of the address range to add to the area.
- *area-id* - Area to which the specified address or range is assigned. An OSPF area identifies a group of routers that share common routing information. (The area ID must be in the form of an IP address.)

Command Mode

Router Configuration

Default Setting

Disabled

Downloaded from www.Manualslib.com manuals search engine

Command Usage

- An area ID uniquely defines an OSPF broadcast area. The area ID 0.0.0.0 indicates the OSPF backbone for an autonomous system. Each router must be connected to the backbone via a direct connection or a virtual link.
- Set the area ID to the same value for all routers on a network segment using the network mask to add one or more interfaces to an area.
- Be sure to include the primary address for an interface in the network area, otherwise, OSPF will not operate for any secondary addresses covered by the command.
- An interface can only be assigned to a single area. If an address range is overlapped in subsequent network area commands, the router will implement the address range for the area specified in first command, and ignore the overlapping ranges in subsequent commands. However, note that if a more specific address range is removed from an area, the interface belonging to that range may still remain active if a less specific address range covering that area has been specified.
- This router supports up to 64 OSPF router interfaces, and up to 16 total areas (either normal transit areas, stubs, or NSSAs).

Example

This example creates the backbone 0.0.0.0 covering class B addresses 10.1.x.x, and a normal transit area 10.2.9.0 covering the class C addresses 10.2.9.x.

```
Console(config-router)#network 10.1.0.0 255.255.0.0 area 0.0.0.0
Console(config-router)#network 10.2.9.0 255.255.255.0 area 10.1.0.0
Console(config-router)#
```

area stub

Use this command to define a stub area. To remove a stub, use the **no** form without the optional keyword. To remove the summary attribute, use the **no** form with the summary keyword.

Syntax

area *area-id* stub [summary]
no area *area-id* **stub** [**summary**]

Downloaded from www.Manualslib.com manuals search engine

- *area-id* - Identifies the stub area.
  (The area ID must be in the form of an IP address.)
- **summary** - Makes an Area Border Router (ABR) send a summary link advertisement into the stub area. (Default: no summary)

Command Mode

Router Configuration

Default Setting

No stub is configured.

Command Usage

- All routers in a stub must be configured with the same area ID.
- Routing table space is saved in a stub by blocking Type-4 AS summary LSAs and Type 5 external LSAs. The default setting for this command completely isolates the stub by blocking Type-3 summary LSAs that advertise the default route for destinations external to the local area or the autonomous system.
- Use the **area default-cost** command to specify the cost of a default summary route sent into a stub by an ABR.
- This router supports up to 16 total areas (either normal transit areas, stubs, or NSSAs).

Example

This example creates a stub area 10.2.0.0, and assigns all interfaces with class B addresses 10.2.x.x to the stub.

```
Console(config-router)#area 10.2.0.0 stub
Console(config-router)#network 10.2.0.0 0.255.255.255 area 10.2.0.0
Console(config-router)#
```

Related Commands

area default-cost (3-152)

Downloaded from www.Manualslib.com manuals search engine

area nssa

Use this command to define a not-so-stubby area (NSSA). To remove an NSSA, use the **no** form without any optional keywords. To remove an optional attribute, use the **no** form without the relevant keyword.

Syntax

area *area-id* nssa [no-redistribution] [default-information-originate]
no area *area-id* **nssa** [**no-redistribution**]
[**default-information-originate**]

- *area-id* - Identifies the NSSA.
  (The area ID must be in the form of an IP address.)
- **no-redistribution** - Use this keyword when the router is an NSSA Area Border Router (ABR) and you want the **redistribute** command to import routes only into normal areas, and not into the NSSA. In other words, this keyword prevents the NSSA ABR from advertising external routing information (learned via routers in other areas) into the NSSA.
- **default-information-originate** - When the router is an NSSA Area Border Router (ABR) or an NSSA Autonomous System Boundary Router (ASBR), this parameter causes it to generate Type-7 default LSA into the NSSA. This default provides a route to other areas within the AS for an NSSA ABR, or to areas outside the AS for an NSSA ASBR.

Command Mode

Router Configuration

Default Setting

No NSSA is configured.

Command Usage

- All routers in a NSSA must be configured with the same area ID.
- An NSSA is similar to a stub, because when the router is an ABR, it can send a default route for other areas in the AS into the NSSA using the **default- information-originate** keyword. However, an NSSA is different from a stub, because when the router is an ASBR, it can

Downloaded from www.Manualslib.com manuals search engine

import a default external AS route (for routing protocol domains adjacent to the NSSA but not within the OSPF AS) into the NSSA using the **default-information-originate** keyword.

- External routes advertised into an NSSA can include network destinations outside the AS learned via OSPF, the default route, static routes, routes imported from other routing protocols such as RIP, and networks directly connected to the router that are not running OSPF.
- NSSA external LSAs (Type 7) are converted by any ABR adjacent to the NSSA into external LSAs (Type-5), and propagated into other areas within the AS.
- Also, note that unlike stub areas, all Type-3 summary LSAs are always imported into NSSAs to ensure that internal routes are always chosen over Type-7 NSSA external routes.
- This router supports up to 16 total areas (either normal transit areas, stubs, or NSSAs).

Example

This example creates a stub area 10.3.0.0, and assigns all interfaces with class B addresses 10.3.x.x to the NSSA. It also instructs the router to generate external LSAs into the NSSA when it is an NSSA ABR or NSSA ASBR.

```
Console(config-router)#area 10.3.0.0 nssa default-information-originate
Console(config-router)#network 10.3.0.0 255.255.0.0 area 10.2.0.0
Console(config-router)#
```


Downloaded from www.Manualslib.com manuals search engine

area virtual-link

Use this command to define a virtual link. To remove a virtual link, use the **no** form with no optional keywords. To restore the default value for an attribute, use the **no** form with the required keyword.

Syntax

area *area-id* virtual-link *router-id*
[authentication [message-digest | null]] [hello-interval *seconds*]
[retransmit-interval *seconds*] [transmit-delay *seconds*] [dead-interval *seconds*]
[[authentication-key *key*] | [message-digest-key *key-id* md5 *key*]]

no area *area-id* **virtual-link** *router-id*
[**authentication** [**message-digest** | **null**]] [**hello-interval** *seconds*]
[**retransmit-interval** *seconds*] [**transmit-delay** *seconds*] [**dead-interval** *seconds*] [[**authentication-key** *key*] | [**message-digest-key** *key-id* **md5** *key*]]

no area *area-id*

- *area-id* - Identifies the transit area for the virtual link. (The area ID must be in the form of an IP address.)
- *router-id* - Router ID of the virtual link neighbor. This must be an Area Border Router (ABR) that is adjacent to both the backbone and the transit area at the other end of the virtual link.
- **authentication** - Specifies the authentication mode. If no optional parameters follow this keyword, then plain text authentication is used along with the password specified by the **authentication-key**. If **message-digest** authentication is specified, then the **message-digest-key** and **md5** parameters must also be specified. If the **null** option is specified, then no authentication is performed on any OSPF routing protocol messages.
- **message-digest** - Specifies message-digest (MD5) authentication.
- **null** - Indicates that no authentication is used.
- **hello-interval** *seconds* - Specifies the transmit delay between sending hello packets. Setting the hello interval to a smaller value can reduce the delay in detecting topological changes, but will increase the routing traffic. This value must be the same for all routers attached to an autonomous system. (Range: 1-65535 seconds; Default: 10 seconds)

Downloaded from www.Manualslib.com manuals search engine

- **retransmit-interval** *seconds* - Specifies the interval at which the ABR retransmits link-state advertisements (LSA) over the virtual link. The retransmit interval should be set to a conservative value that provides an adequate flow of routing information, but does not produce unnecessary protocol traffic. However, note that this value should be larger for virtual links. (Range: 1-3600 seconds; Default: 5 seconds)
- **transmit-delay** *seconds* - Estimates the time required to send a link-state update packet over the virtual link, considering the transmission and propagation delays. LSAs have their age incremented by this amount before transmission. This value must be the same for all routers attached to an autonomous system. (Range: 1-3600 seconds; Default: 1 seconds)
- **dead-interval** *seconds* - Specifies the time that neighbor routers will wait for a hello packet before they declare the router down. This value must be the same for all routers attached to an autonomous system. (Range: 1-65535 seconds; Default: 4 x hello interval, or 40 seconds)
- **authentication-key** *key* - Sets a plain text password (up to 8 characters) that is used by neighboring routers on a virtual link to generate or verify the authentication field in protocol message headers. A separate password can be assigned to each network interface. However, this key must be the same for all neighboring routers on the same network (i.e., autonomous system). This key is only used when authentication is enabled for the backbone.
- **message-digest-key** *key-id* **md5** *key* - Sets the key identifier and password to be used to authenticate protocol messages passed between neighboring routers and this router when using message digest (MD5) authentication. The *key-id* is an integer from 1-255, and the *key* is an alphanumeric string up to 16 characters long. If MD5 authentication is used on a virtual link, then it must be enabled on all routers within an autonomous system; and the key identifier and key must also be the same for all routers.

Command Mode

Router Configuration

Downloaded from www.Manualslib.com manuals search engine

Default Setting

area-id: None
router-id: None
hello-interval: 10 seconds
retransmit-interval: 5 seconds
transmit-delay: 1 second
dead-interval: 40 seconds
authentication-key: None
message-digest-key: None

Command Usage

- All areas must be connected to a backbone area (0.0.0.0) to maintain routing connectivity throughout the autonomous system. If it not possible to physically connect an area to the backbone, you can use a virtual link. A virtual link can provide a logical path to the backbone for an isolated area. You can specify up to 32 virtual links on this router.
- Any area disconnected from the backbone must include the transit area ID and the router ID for a virtual link neighbor that is adjacent to the backbone.
- This router supports up 64 virtual links.

Example

This example creates a virtual link using the defaults for all optional parameters.

```
Console(config-router)#network 10.4.0.0 0.255.255.0.0 area 10.4.0.0
Console(config-router)#area 10.4.0.0 virtual-link 10.4.3.254
Console(config-router)#
```

This example creates a virtual link using MD5 authentication.

```
Console(config-router)#network 10.4.0.0 0.255.255.0.0 area 10.4.0.0
Console(config-router)#area 10.4.0.0 virtual-link 10.4.3.254
message-digest-key 5 md5 ld83jdpq
Console(config-router)#
```

Related Commands

show ip ospf virtual-links (3-184)

Downloaded from www.Manualslib.com manuals search engine

ip ospf authentication

Use this command to specify the authentication type used for an interface. Enter this command without any optional parameters to specify plain text (or simple password) authentication. Use the **no** form to restore the default of no authentication.

Syntax

ip ospf authentication [**message-digest** | **null**]
no ip ospf authentication

- **message-digest** - Specifies message-digest (MD5) authentication.
- **null** - Indicates that no authentication is used.

Command Mode

Interface Configuration (VLAN)

Default Setting

No authentication

Command Usage

- Before specifying plain-text password authentication for an interface, configure a password with the **ip ospf authentication-key** command. Before specifying MD5 authentication for an interface, configure the message-digest key-id and key with the **ip ospf message-digest-key** command.
- The plain-text authentication-key, or the MD5 key-id and key, must be used consistently throughout the autonomous system.

Example

This example enables message-digest authentication for the specified interface.

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf authentication message-digest
Console(config-if)#
```

Related Commands

ip ospf authentication-key (3-164)
ip ospf message-digest-key (3-165)

Downloaded from www.Manualslib.com manuals search engine

ip ospf authentication-key

Use this command to assign a simple password to be used by neighboring routers. Use the **no** form to remove the password.

Syntax

ip ospf authentication-key *key*
no ip ospf authentication-key

key - Sets a plain text password. (Range: 1-8 characters)

Command Mode

Interface Configuration (VLAN)

Default Setting

No password

Command Usage

- Before specifying plain-text password authentication for an interface, configure a password with the **ip ospf authentication-key** command. Before specifying MD5 authentication for an interface, configure the message-digest key-id and key with the **ip ospf message-digest-key** command.
- A different password can be assigned to each network interface basis, but the password must be used consistently on all neighboring routers throughout a network (i.e., autonomous system).

Example

This example sets a password for the specified interface.

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf authentication-key badboy
Console(config-if)#
```

Related Commands

ip ospf authentication (3-163)

Downloaded from www.Manualslib.com manuals search engine

ip ospf message-digest-key

Use this command to enable message-digest (MD5) authentication on the specified interface and to assign a key-id and key to be used by neighboring routers. Use the **no** form to remove an existing key.

Syntax

ip ospf message-digest-key *key-id* **md5** *key*
no ip ospf message-digest-key *key-id*

- *key-id* - Index number of an MD5 key. (Range: 1-255)
- *key* - Alphanumeric password used to generate a 128 bit message digest or "fingerprint." (Range: 1-16 characters)

Command Mode

Interface Configuration (VLAN)

Default Setting

MD5 authentication is disabled.

Command Usage

- Normally, only one key is used per interface to generate authentication information for outbound packets and to authenticate incoming packets. Neighbor routers must use the same key identifier and key value.
- When changing to a new key, the router will send multiple copies of all protocol messages, one with the old key and another with the new key. Once all the neighboring routers start sending protocol messages back to this router with the new key, the router will stop using the old key. This rollover process gives the network administrator time to update all the routers on the network without affecting the network connectivity. Once all the network routers have been updated with the new key, the old key should be removed for security reasons.

Example

This example sets a message-digest key identifier and password.

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf message-digest-key 1 md5 aiebel
Console(config-if)#
```


Downloaded from www.Manualslib.com manuals search engine

Related Commands

ip ospf authentication (3-163)

ip ospf cost

Use this command to explicitly set the cost of sending a packet on an interface. Use the **no** form to restore the default value.

Syntax

ip ospf cost *cost*
no ip ospf cost

cost - Link metric for this interface. Use higher values to indicate slower ports. (Range: 1-65535)

Command Mode

Interface Configuration (VLAN)

Default Setting

1

Command Usage

Interface cost reflects the port speed. This router uses a default cost of 1 for all ports. Therefore, if you install a Gigabit module, you may have to reset the cost for all of the 100 Mbps ports to a value greater than 1.

Example

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf cost 10
Console(config-if)#
```

ip ospf dead-interval

Use this command to set the interval at which hello packets are not seen before neighbors declare the router down. Use the **no** form to restore the default value.

Syntax

ip ospf dead-interval *seconds*
no ip ospf dead-interval

Downloaded from www.Manualslib.com manuals search engine

seconds - The maximum time that neighbor routers can wait for a hello packet before declaring the transmitting router down. This interval must be set to the same value for all routers on the network. (Range: 1-65535)

Command Mode

Interface Configuration (VLAN)

Default Setting

40, or four times the interval specified by the **ip ospf hello-interval** command.

Example

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf dead-interval 50
Console(config-if)#
```

Related Commands

ip ospf hello-interval (3-167)

ip ospf hello-interval

Use this command to specify the interval between sending hello packets on an interface. Use the **no** form to restore the default value.

Syntax

ip ospf hello-interval *seconds*
no ip ospf hello-interval

seconds - Interval at which hello packets are sent from an interface. This interval must be set to the same value for all routers on the network. (Range: 1-65535)

Command Mode

Interface Configuration (VLAN)

Default Setting

10 seconds

Command Usage

Hello packets are used to inform other routers that the sending router is still active. Setting the hello interval to a smaller value can reduce the delay in detecting topological changes, but will increase routing traffic.

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf hello-interval 5
Console(config-if)#
```

ip ospf priority

Use this command to set the router priority used when determining the designated router (DR) and backup designated router (BDR) for an area. Use the **no** form to restore the default value.

Syntax

ip ospf priority *priority*
no ip ospf priority

priority - Sets the interface priority for this router. (Range: 0-255)

Command Mode

Interface Configuration (VLAN)

Default Setting

1

Command Usage

- Set the priority to zero to prevent a router from being elected as a DR or BDR. If set to any value other than zero, the router with the highest priority will become the DR and the router with the next highest priority becomes the BDR. If two or more routers are tied with the same highest priority, the router with the higher ID will be elected.
- If a DR already exists for an area when this interface comes up, the new router will accept the current DR regardless of its own priority. The DR will not change until the next time the election process is initiated.

Example

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf priority 5
Console(config-if)#
```


Downloaded from www.Manualslib.com manuals search engine

ip ospf retransmit-interval

Use this command to specify the time between resending link-state advertisements (LSAs). Use the **no** form to restore the default value.

Syntax

ip ospf retransmit-interval *seconds*
no ip ospf retransmit-interval

seconds - Sets the interval at which LSAs are retransmitted from this interface. (Range: 1-65535)

Command Mode

Interface Configuration (VLAN)

Default Setting

5 seconds

Command Usage

A router will resend an LSA to a neighbor if it receives no acknowledgment. The retransmit interval should be set to a conservative value that provides an adequate flow of routing information, but does not produce unnecessary protocol traffic. Note that this value should be larger for virtual links.

Example

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf retransmit-interval 7
Console(config-if)#
```

ip ospf transmit-delay

Use this command to set the estimated time to send a link-state update packet over an interface. Use the **no** form to restore the default value.

Syntax

ip ospf transmit-delay *seconds*
no ip ospf transmit-delay

seconds - Sets the estimated time required to send a link-state update. (Range: 1-65535)

Downloaded from www.Manualslib.com manuals search engine

Command Mode

Interface Configuration (VLAN)

Default Setting

1 second

Command Usage

LSAs have their age incremented by this delay before transmission. When estimating the transmit delay, consider both the transmission and propagation delays for an interface. Set the transmit delay according to link speed, using larger values for lower-speed links. The transmit delay must be the same for all routers attached to an autonomous system.

Example

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf transmit-delay 6
Console(config-if)#
```

show ip ospf

Use this command to show basic information about the routing configuration.

Command Mode

Privileged Exec

Example

```
Console#show ip ospf
Routing Process with ID 10.1.1.253
Supports only single TOS(TOS0) route
It is an area border and autonomous system boundary router
Redistributing External Routes from,
     rip with metric mapped to 10
Number of area in this router is 2
Area 0.0.0.0 (BACKBONE)
     Number of interfaces in this area is 1
     SPF algorithm executed 19 times
Area 10.1.0.0
     Number of interfaces in this area is 4
     SPF algorithm executed 19 times
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Field	Description
Routing Process with ID	Router ID
Supports only single TOS (TOS0) route	Type of service is not supported, so you can only assign one cost per interface
It is an *router type*	The types displayed include internal, area border, or autonomous system boundary routers
Number of areas in this router	The number of configured areas
Area *identifier*	The area address, and area type if backbone, NSSA or stub
Number of interfaces	The number of interfaces attached to this area
SPF algorithm executed	The number of times the shortest path first algorithm has been executed for this area

show ip ospf border-routers

Use this command to show entries in the routing table that lead to an Area Border Router (ABR) or Autonomous System Boundary Router (ASBR).

Command Mode

Privileged Exec

Example

```
Console#show ip ospf border-routers

  Destination      Next Hop      Cost   Type  RteType      Area         SPF No
--------------- --------------- ------ ----- -------- ---------------
-------
     10.1.1.252      10.1.1.253      0   ABR    INTRA        10.1.0.0       3
     10.2.6.252      10.2.9.253      0   ASBR   INTER        10.2.0.0       7
Console#
```

Field	Description
Destination	Identifier for the destination router
Next Hop	IP address of the next hop toward the destination
Cost	Link metric for this route
Type	Router type of the destination; either ABR, ASBR or both
RteType	Route type; either intra-area or interarea route (INTRA or INTER)

Downloaded from www.Manualslib.com manuals search engine

Field	Description
Area	The area from which this route was learned
SPF No	The number of times the shortest path first algorithm has been executed for this route

show ip ospf database

Use this command to show information about different OSPF Link State Advertisements (LSAs) stored in this router's database.

Syntax

show ip ospf [*area-id*] **database** [**adv-router** [*ip-address*]]

show ip ospf [*area-id*] **database** [**asbr-summary**] [*link-state-id*]
show ip ospf [*area-id*] **database** [**asbr-summary**] [*link-state-id*] [**adv-router** [*ip-address*]]
show ip ospf [*area-id*] **database** [**asbr-summary**] [*link-state-id*] [**self-originate**] [*link-state-id*]

show ip ospf [*area-id*] **database** [**database-summary**]

show ip ospf [*area-id*] **database** [**external**] [*link-state-id*]
show ip ospf [*area-id*] **database** [**external**] [*link-state-id*] [**adv-router** [*ip-address*]]
show ip ospf [*area-id*] **database** [**external**] [*link-state-id*] [**self-originate**] [*ip-address*]

show ip ospf [*area-id*] **database** [**network**] [*link-state-id*]
show ip ospf [*area-id*] **database** [**network**] [*link-state-id*] [**adv-router** [*ip-address*]]
show ip ospf [*area-id*] **database** [**network**] [*link-state-id*] [**self-originate**] [*link-state-id*]

show ip ospf [*area-id*] **database** [**nssa-external**] [*link-state-id*]
show ip ospf [*area-id*] **database** [**nssa-external**] [*link-state-id*] [**adv-router** [*ip-address*]]
show ip ospf [*area-id*] **database** [**nssa-external**] [*link-state-id*] [**self-originate**] [*link-state-id*]

show ip ospf [*area-id*] **database** [**router**] [*link-state-id*]
show ip ospf [*area-id*] **database** [[**router**] [**adv-router** [*ip-address*]]
show ip ospf [*area-id*] **database** [**router**] [**self-originate**] [*link-state-id*]

show ip ospf [*area-id*] **database** [**self-originate**] [*link-state-id*]

show ip ospf [*area-id*] **database** [**summary**] [*link-state-id*]
show ip ospf [*area-id*] **database** [**summary**] [*link-state-id*] [**adv-router** [*ip-address*]]
show ip ospf [*area-id*] **database** [**summary**] [*link-state-id*] [**self-originate**] [*link-state-id*]

- *area-id* - Area defined for which you want to view LSA information. (This item must be entered in the form of an IP address.)
- **adv-router** - IP address of the advertising router. If not entered, information about all advertising routers is displayed.
- *ip-address* - IP address of the specified router. If no address is entered, information about the local router is displayed.
- **asbr-summary** - Shows information about Autonomous System Boundary Router summary LSAs.
- *link-state-id* - The network portion described by an LSA. The *link-state-id* entered should be:

Downloaded from www.Manualslib.com manuals search engine

- An IP network number for Type 3 Summary and External LSAs
- A Router ID for Router, Network, and Type 4 AS Summary LSAs

Also, note that when an Type 5 ASBR External LSA is describing a default route, its *link-state-id* is set to the default destination (0.0.0.0).

- **self-originate** - Shows LSAs originated by this router.
- **database-summary** - Shows a count for each LSA type for each area stored in the database, and the total number of LSAs in the database.
- **external** - Shows information about external LSAs.
- **network** - Shows information about network LSAs.
- **nssa-external** - Shows information about NSSA external LSAs.
- **router** - Shows information about router LSAs.
- **summary** - Shows information about summary LSAs.

Command Mode

Privileged Exec

Examples

The following shows output for the **show ip ospf database** command.

```
Console#show ip ospf database


     Displaying Router Link States(Area 10.1.0.0)
       Link ID      ADV Router    Age      Seq#     Checksum
--------------- --------------- ------ ----------- -----------
     10.1.1.252      10.1.1.252     26  0X80000005      0X89A1
     10.1.1.253      10.1.1.253     23  0X80000002      0X8D9D


     Displaying Net Link States(Area 10.1.0.0)
       Link ID      ADV Router    Age      Seq#     Checksum
--------------- --------------- ------ ----------- -----------
     10.1.1.252      10.1.1.252     28  0X80000001      0X53E1
Console#
```

Field	Description
Link ID	Router ID
ADV Router	Advertising router ID
Age	Age of LSA (in seconds)
Seq#	Sequence number of LSA (used to detect older duplicate LSAs)
Checksum	Checksum of the complete contents of the LSA

Downloaded from www.Manualslib.com manuals search engine

The following shows output when using the **asbr-summary** keyword.

```
Console#show ip ospf database asbr-summary

OSPF Router with id(10.1.1.253)

          Displaying Summary ASB Link States(Area 0.0.0.0)


LS age: 433
Options: (No TOS-capability)
LS Type: Summary Links (AS Boundary Router)
Link State ID: 192.168.5.1 (AS Boundary Router's Router ID)
Advertising Router: 192.168.1.5
LS Sequence Number: 80000002
LS Checksum: 0x51E2
Length: 32
Network Mask: 255.255.255.0
Metric: 1

Console#
```

Field	Description
OSPF Router id	Router ID
LS age	Age of LSA (in seconds)
Options	Optional capabilities associated with the LSA
LS Type	Summary Links - LSA describes routes to AS boundary routers
Link State ID	Interface address of the autonomous system boundary router
Advertising Router	Advertising router ID
LS Sequence Number	Sequence number of LSA (used to detect older duplicate LSAs)
LS Checksum	Checksum of the complete contents of the LSA
Length	The length of the LSA in bytes
Network Mask	Address mask for the network
Metrics	Cost of the link

Downloaded from www.Manualslib.com manuals search engine

The following shows output when using the **database-summary** keyword.

```
Console#show ip ospf database database-summary


Area ID (10.1.0.0)
     Router    Network    Sum-Net    Sum-ASBR    External-AS    External-Nssa
          2          1          1           0              0                0
Total LSA Counts : 4
Console#
```

Field	Description
Area ID	Area identifier
Router	Number of router LSAs
Network	Number of network LSAs
Sum-Net	Number of summary LSAs
Sum-ASBR	Number of summary ASBR LSAs
External-AS	Number of autonomous system external LSAs
External-Nssa	Number of NSSA external network LSAs
Total LSA Counts	Total number of LSAs

Downloaded from www.Manualslib.com manuals search engine

The following shows output when using the **external** keyword.

```
Console#show ip ospf database external

OSPF Router with id(192.168.5.1) (Autonomous system 5)

          Displaying AS External Link States


LS age: 433
Options: (No TOS-capability)
LS Type: AS External Link
Link State ID: 10.1.1.253 (External Network Number)
Advertising Router: 10.1.2.254
LS Sequence Number: 80000002
LS Checksum: 0x51E2
Length: 32
Network Mask: 255.255.0.0
Metric Type: 2 (Larger than any link state path)
Metric: 1
Forward Address: 0.0.0.0
External Route Tag: 0

Console#
```

Field	Description
OSPF Router id	Router ID
LS age	Age of LSA (in seconds)
Options	Optional capabilities associated with the LSA
LS Type	AS External Links - LSA describes routes to destinations outside the AS (including default external routes for the AS)
Link State ID	IP network number (External Network Number)
Advertising Router	Advertising router ID
LS Sequence Number	Sequence number of LSA (used to detect older duplicate LSAs)
LS Checksum	Checksum of the complete contents of the LSA
Length	The length of the LSA in bytes
Network Mask	Address mask for the network
Metric Type	Type 1 or Type 2 external metric (see "redistribute" on page 3-154)
Metrics	Cost of the link

Downloaded from www.Manualslib.com manuals search engine

Field	Description
Forward Address	Forwarding address for data to be passed to the advertised destination (If set to 0.0.0.0, data is forwarded to the originator of the advertisement)
External Route Tag	32-bit field attached to each external route (Not used by OSPF; may be used to communicate other information between boundary routers as defined by specific applications)

The following shows output when using the **network** keyword.

```
Console#show ip ospf database network

OSPF Router with id(10.1.1.253)

          Displaying Net Link States(Area 10.1.0.0)


Link State Data Network (Type 2)
--------------------------------

LS age: 433
Options: Support External routing capability
LS Type: Network Links
Link State ID: 10.1.1.252 (IP interface address of the Designated Router)
Advertising Router: 10.1.1.252
LS Sequence Number: 80000002
LS Checksum: 0x51E2
Length: 32
Network Mask: 255.255.255.0

       Attached Router: 10.1.1.252
       Attached Router: 10.1.1.253
Console#
```

Field	Description
OSPF Router id	Router ID
LS age	Age of LSA (in seconds)
Options	Optional capabilities associated with the LSA
LS Type	Network Link - LSA describes the routers attached to the network
Link State ID	Interface address of the designated router
Advertising Router	Advertising router ID

Downloaded from www.Manualslib.com manuals search engine

Field	Description
LS Sequence Number	Sequence number of LSA (used to detect older duplicate LSAs)
LS Checksum	Checksum of the complete contents of the LSA
Length	The length of the LSA in bytes
Network Mask	Address mask for the network
Attached Router	List of routers attached to the network; i.e., fully adjacent to the designated router, including the designated router itself

The following shows output when using the **router** keyword.

```
Console#show ip ospf database router

OSPF Router with id(10.1.1.253)

          Displaying Router Link States(Area 10.1.0.0)


Link State Data Router (Type 1)
-------------------------------

LS age: 233
Options: Support External routing capability
LS Type: Router Links
Link State ID: 10.1.1.252 (Originating Router's Router ID)
Advertising Router: 10.1.1.252
LS Sequence Number: 80000011
LS Checksum: 0x7287
Length: 48
Router Role: Area Border Router
Number of Links: 1
-----------------------------------------------------
Link ID:  10.1.7.0 (IP Network/Subnet Number)
   Link Data: 255.255.255.0 (Network's IP address mask)
   Link Type: Connection to a stub network
   Number of TOS metrics: 0
   Metrics: 1

Console#
```

Field	Description
OSPF Router id	Router ID
LS age	Age of LSA (in seconds)
Options	Optional capabilities associated with the LSA
LS Type	Router Link - LSA describes the router's interfaces.

Downloaded from www.Manualslib.com manuals search engine

Field	Description
Link State ID	Router ID of the router that originated the LSA
Advertising Router	Advertising router ID
LS Sequence Number	Sequence number of LSA (used to detect older duplicate LSAs)
LS Checksum	Checksum of the complete contents of the LSA
Length	The length of the LSA in bytes
Router Role	Description of router type, including: None, AS Boundary Router, Area Border Router, or Virtual Link
Number of Links	Number of links described by the LSA
Link ID	Link type and corresponding Router ID or network address
Link Data	• Router ID for transit network • Network's IP address mask for stub network • Neighbor Router ID for virtual link
Link Type	Link-state type, including transit network, stub network, or virtual link
Number of TOS metrics	Type of Service metric – This router only supports TOS 0 (or normal service)
Metrics	Cost of the link

Downloaded from www.Manualslib.com manuals search engine

The following shows output when using the **summary** keyword.

```
Console#show ip ospf database summary

OSPF Router with id(10.1.1.253)

          Displaying Summary Net Link States(Area 10.1.0.0)


Link State Data Summary (Type 3)
--------------------------------

LS age: 686
Options: Support External routing capability
LS Type: Summary Links(Network)
Link State ID: 10.2.6.0 (The destination Summary Network Number)
Advertising Router: 10.1.1.252
LS Sequence Number: 80000003
LS Checksum: 0x3D02
Length: 28
Network Mask: 255.255.255.0
Metric: 1

Console#
```

Field	Description
OSPF Router id	Router ID
LS age	Age of LSA (in seconds)
Options	Optional capabilities associated with the LSA
LS Type	Summary Links - LSA describes routes to networks
Link State ID	Router ID of the router that originated the LSA
Advertising Router	Advertising router ID
LS Sequence Number	Sequence number of LSA (used to detect older duplicate LSAs)
LS Checksum	Checksum of the complete contents of the LSA
Length	The length of the LSA in bytes
Network Mask	Destination network's IP address mask
Metrics	Cost of the link

Downloaded from www.Manualslib.com manuals search engine

show ip ospf interface

Use this command to display summary information for OSPF interfaces.

Syntax

show ip ospf interface [**vlan** *vlan-id*]

vlan-id - VLAN ID (Range: 1-4094)

Command Mode

Privileged Exec

Example

```
Console#show ip ospf interface vlan 1

Vlan 1 is up
  Interface Address 10.1.1.253, Mask 255.255.255.0, Area 10.1.0.0
  Router ID 10.1.1.253, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router id 10.1.1.252, Interface address 10.1.1.252
  Backup Designated router id 10.1.1.253, Interface addr 10.1.1.253
  Timer intervals configured, Hello 10, Dead 40, Retransmit 5

Console#
```

Field	Description
Vlan	VLAN ID and Status of physical link
Interface Address	IP address of OSPF interface
Mask	Network mask for interface address
Area	OSPF area to which this interface belongs
Router ID	Router ID
Network Type	Includes broadcast, non-broadcast, or point-to-point networks
Cost	Interface transmit cost
Transmit Delay	Interface transmit delay (in seconds)

Downloaded from www.Manualslib.com manuals search engine

Field	Description
State	• Disabled – OSPF not enabled on this interface • Down – OSPF is enabled on this interface, but interface is down • Loopback – This is a loopback interface • Waiting – Router is trying to find the DR and BDR • DR – Designated Router • BDR – Backup Designated Router • DRother – Interface is on a multiaccess network, but is not the DR or BDR
Priority	Router priority
Designated Router	Designated router ID and respective interface address
Backup Designated Router	Backup designated router ID and respective interface address
Timer intervals	Configuration settings for timer intervals, including Hello, Dead and Retransmit

show ip ospf neighbor

Use this command to display information about neighboring routers on each interface within an OSPF area.

Syntax

show ip ospf neighbor

Command Mode

Privileged Exec

Example

```
Console#show ip ospf neighbor

      ID          Pri        State          Address
--------------- ------ ---------------- ---------------
     10.1.1.252      1          FULL/DR      10.1.1.252

Console#
```

Field	Description
ID	Neighbor's router ID
Pri	Neighbor's router priority

Downloaded from www.Manualslib.com manuals search engine

Field	Description
State	OSPF state and identification flag States include: Down – Connection down Attempt – Connection down, but attempting contact (for non-broadcast networks) Init – Have received Hello packet, but communications not yet established Two-way – Bidirectional communications established ExStart – Initializing adjacency between neighbors Exchange – Database descriptions being exchanged Loading – LSA databases being exchanged Full – Neighboring routers now fully adjacent Identification flags include: D – Dynamic neighbor S – Static neighbor DR – Designated router BDR – Backup designated router
Address	IP address of this interface

show ip ospf summary-address

Use this command to display all summary address information.

Syntax

show ip ospf summary-address

Command Mode

Privileged Exec

Example

This example shows a summary address and associated network mask.

```
Console#show ip ospf summary-address
10.1.0.0/255.255.0.0
Console#
```

Related Commands

summary-address (3-153)

Downloaded from www.Manualslib.com manuals search engine

show ip ospf virtual-links

Use this command to display detailed information about virtual links.

Syntax

show ip ospf virtual-links

Command Mode

Privileged Exec

Example

```
Console#show ip ospf virtual-links
Virtual Link to router 10.1.1.253 is up
Transit area 10.1.1.0
Transmit Delay is 1 sec
Timer intervals configured, Hello 10, Dead 40, Retransmit 5
Console#
```

Field	Description
Virtual Link to router	OSPF neighbor and link state (up or down)
Transit area	Common area the virtual link crosses to reach the target router
Transmit Delay	Estimated transmit delay (in seconds) on the virtual link
Timer intervals	Configuration settings for timer intervals, including Hello, Dead and Retransmit

Related Commands

area virtual-link (3-160)

Multicast Routing Commands

This router uses IGMP snooping and query to determine the ports connected to downstream multicast hosts, and to propagate this information back up through the multicast tree to ensure that requested services are forwarded through each intermediate node between the multicast server and its hosts, and also to filter traffic from all of the other interfaces that do not require these services.

Downloaded from www.Manualslib.com manuals search engine

Multicast routers use snooping and query messages, along with a multicast routing protocol to deliver IP multicast packets across different subnetworks. This router supports both the Distance-Vector Multicast Routing Protocol (DVMRP) and Protocol Independent Multicasting (PIM). (Note that you should enable IGMP for any interface that is using multicast routing.)

Command Groups	Function	Page
Static Multicast Routing	Configures static multicast router ports	3-185
General Multicast Routing	Enables IP multicast routing globally; also displays the IP multicast routing table created from static and dynamic routing information	3-187
DVMRP Multicast Routing	Configures global and interface settings for DVMRP	3-191
PIM-DM Multicast Routing	Configures global and interface settings for PIM-DM	3-202

Static Multicast Routing Commands

Command	Function	Mode	Page
ip igmp snooping vlan mrouter	Adds a multicast router port	GC	3-185
show ip igmp snooping mrouter	Shows multicast router ports	PE	3-186

ip igmp snooping vlan mrouter

Use this command to statically configure a multicast router port. Use the **no** form to remove the configuration.

Syntax

ip igmp snooping vlan *vlan-id* **mrouter** *interface*
no ip igmp snooping vlan *vlan-id* **mrouter** *interface*

- *vlan-id* - VLAN ID (Range: 1-4094)

Downloaded from www.Manualslib.com manuals search engine

- *interface*
  - **ethernet** *unit/port*
    - *unit* - This is device 1.
    - *port* - Port number.
  - **port-channel** *channel-id* (Range: 1-6)

Default Setting

No static multicast router ports are configured.

Command Mode

Global Configuration

Command Usage

Depending on your network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router/switch connected over the network to an interface (port or trunk) on your router, you can manually configure that interface to join all the current multicast groups.

Example

The following shows how to configure port 11 as a multicast router port within VLAN 1:

```
Console(config)#ip igmp snooping vlan 1 mrouter ethernet 1/11
Console(config)#
```

show ip igmp snooping mrouter

Use this command to display information on statically configured and dynamically learned multicast router ports.

Syntax

show ip igmp snooping mrouter [**vlan** *vlan-id*]

vlan-id - VLAN ID (Range: 1-4094)

Downloaded from www.Manualslib.com manuals search engine

Default Setting

Displays multicast router ports for all configured VLANs.

Command Mode

Privileged Exec

Command Usage

Multicast router port types displayed include Static or Dynamic.

Example

The following shows that port 11 in VLAN 1 is attached to a multicast router:

```
Console#show ip igmp snooping mrouter vlan 1
 VLAN M'cast Router Ports Type
 ---- ------------------- -------
    1            Eth 1/11  Static
    2            Eth 1/12  Dynamic
Console#
```

General Multicast Routing Commands

Command	Function	Mode	Page
ip multicast-routing	Enables IP multicast routing	GC	3-187
show ip mroute	Shows the IP multicast routing table	PE	3-188

ip multicast-routing

Use this command to enable IP multicast routing. Use the **no** form to disable IP multicast routing.

Syntax

ip multicast-routing
no ip multicast-routing

Default Setting

Disabled

Downloaded from www.Manualslib.com manuals search engine

Command Mode

Global Configuration

Command Usage

This command is used to enable multicast routing globally for the router. You also need to globally enable a specific multicast routing protocol using the **router dvmrp** or **router pim** command, and then specify the interfaces that will support multicast routing using the **ip dvmrp** or **ip pim dense-mode** commands.

Example

```
Console(config)#ip multicast-routing
Console(config)#
```

show ip mroute

Use this command to display the IP multicast routing table.

Syntax

show ip mroute [*group-address source*] [**summary**]

- *group-address* - An IP multicast group address with subscribers directly attached or downstream from this router.
- *source* - The IP subnetwork at the root of the multicast delivery tree. This subnetwork contains a known multicast source.
- **summary** - Displays summary information for each entry in the IP multicast routing table.

Command Mode

Privileged Exec

Command Usage

This command displays information for multicast routing. If no optional parameters are selected, detailed information for each entry in the multicast address table is displayed. If you select a multicast group

Downloaded from www.Manualslib.com manuals search engine

and source pair, detailed information is displayed only for the specified entry. If the **summary** option is selected, an abbreviated list of information for each entry is displayed on a single line.

Example

This example shows detailed multicast information for a specified group/ source pair

```
Console#show ip mroute 224.0.255.3 192.111.46.8
IP Multicast Forwarding is enabled.

IP Multicast Routing Table

Flags:  P - Prune, F - Forwarding
(192.111.46.0, 255.255.255.0, 224.0.255.3)
Owner: DVMPR
Upstream Interface: vlan1
Upstream Router: 148.122.34.9
Downstream: vlan2(P), vlan3(F)
Console#
```

Field	Description
Source and netmask	Subnetwork containing the IP multicast source.
Group address	IP multicast group address for a requested service.
Owner	The associated multicast protocol (i.e., DVMRP or PIM-DM).
Upstream Interface	Interface leading to the upstream neighbor.
Upstream Router	IP address of the multicast router immediately upstream for this group.
Downstream interface and flags	The interface(s) on which multicast subscribers have been recorded. The flags associated with each interface indicate prune (P) if the downstream interface has been recently terminated or forwarding (F) if the interface is still active.

Downloaded from www.Manualslib.com manuals search engine

This example lists all entries in the multicast table in summary form:

```
Console#show ip mroute summary
IP Multicast Forwarding is enabled.

IP Multicast Routing Table (Summary)

Flags:  P - Prune UP

     Group           Source        Source Mask    Interface  Owner   Flags
--------------- --------------- --------------- ---------- ------- ------
       224.1.1.1      10.1.0.0      255.255.0.0      vlan1   DVMRP       P
       224.2.2.2      10.1.0.0      255.255.0.0      vlan1   DVMRP      --
Console#
```


Downloaded from www.Manualslib.com manuals search engine

DVMRP Multicast Routing Commands

Command	Function	Mode	Page
router dvmrp	Enables DVMRP and enters router configuration mode	GC	3-191
probe-interval	Sets the interval for sending neighbor probe messages	RC	3-192
nbr-timeout	Sets the delay before declaring an attached neighbor router down	RC	3-193
report-interval	Sets the interval for propagating the complete set of routing tables to other neighbor routers	RC	3-194
flash-update-interval	Sets the interval for sending updates about changes to network topology	RC	3-194
prune-lifetime	Defines how long a prune state remains in effect for a source-routed multicast tree	RC	3-195
default-gateway	Configures the default gateway for IP multicast routing	RC	3-196
ip dvmrp	Enables DVMRP on the specified interface	IC	3-197
ip dvmrp metric	Sets the metric used when establishing reverse paths to some networks on directly attached interfaces	IC	3-198
clear ip dvmrp route	Clears all dynamic routes in the multicast routing table	PE	3-198
show router dvmrp	Displays global DVMRP configuration settings	NE, PE	3-199
show ip dvmrp route	Displays DVMRP routing information	NE, PE	3-200
show ip dvmrp neighbor	Displays DVMRP neighbor information	NE, PE	3-201
show ip dvmrp interface	Displays DVMRP configuration settings for the interfaces	NE, PE	3-202

router dvmrp

Use this command to enable Distance-Vector Multicast Routing (DVMRP) globally for the router and to enter router configuration mode. Use the **no** form to disable DVMRP multicast routing.

Downloaded from www.Manualslib.com manuals search engine

Syntax

router dvmrp
no router dvmrp

Command Mode

Global Configuration

Command Usage

This command enables DVMRP globally for the router and enters router configuration mode. Make any changes necessary to the global DVMRP parameters. Then specify the interfaces that will support DVMRP multicast routing using the **ip dvmrp** command, and set the metric for each interface.

Example

```
Console(config)#router dvmrp
Console(config-router)#end
Console#show router dvmrp
Admin Status                    : enable
Probe Interval                  : 10
Nbr expire                      : 35
Minimum Flash Update Interval   : 5
prune lifetime                  : 7200
route report                    : 60
Default Gateway                 : 0.0.0.0
Metric of Default Gateway       : 0
Console#
```

Related Commands

ip dvmrp (3-197)
show router dvmrp (3-199)

probe-interval

Use this command to set the interval for sending neighbor probe messages to the multicast group address for all DVMRP routers. Use the **no** form to restore the default value.

Syntax

probe-interval *seconds*

Downloaded from www.Manualslib.com manuals search engine

seconds - Interval between sending neighbor probe messages. (Range: 1-65535)

Default Setting

10 seconds

Command Mode

Router Configuration

Command Usage

Probe messages are sent to neighboring DVMRP routers from which this device has received probes, and is used to verify whether or not these neighbors are still active members of the multicast tree.

Example

```
Console(config-router)#probe-interval 30
Console(config-router)#
```

nbr-timeout

Use this command to set the interval to wait for messages from a DVMRP neighbor before declaring it dead. Use the **no** form to restore the default value.

Syntax

nbr-timeout *seconds*

seconds - Interval before declaring a neighbor dead. (Range: 1-65535)

Default Setting

35 seconds

Command Mode

Router Configuration

Command Usage

This command is used for timing out routes, and for setting the children and leaf flags.

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console(config-router)#nbr-timeout 40
Console(config-router)#
```

report-interval

Use this command to specify how often to propagate the complete set of routing tables to other neighbor DVMRP routers. Use the **no** form to restore the default value.

Syntax

report-interval *seconds*

seconds - Interval between sending the complete set of routing tables. (Range: 1-65535)

Default Setting

60 seconds

Command Mode

Router Configuration

Example

```
Console(config-router)#report-interval 90
Console(config-router)#
```

flash-update-interval

Use this command to specify how often to send trigger updates, which reflect changes in the network topology. Use the **no** form to restore the default value.

Syntax

flash-update-interval *seconds*

seconds - Interval between sending flash updates when network topology changes have occurred. (Range: 1-65535)

Downloaded from www.Manualslib.com manuals search engine

Default Setting

5 seconds

Command Mode

Router Configuration

Example

```
Console(config-router)#flash-update-interval 10
Console(config-router)#
```

prune-lifetime

Use this command to specify how long a prune state will remain in effect for a multicast tree. Use the **no** form to restore the default value.

Syntax

prune-lifetime *seconds*

seconds - Prune state lifetime. (Range: 1-65535)

Default Setting

7200 seconds

Command Mode

Router Configuration

Command Usage

This command sets the prune state lifetime. After the prune state expires, the router will resume flooding multicast traffic from the multicast source device.

Example

```
Console(config-router)#prune-lifetime 5000
Console(config-router)#
```


Downloaded from www.Manualslib.com manuals search engine

default-gateway

Use this command to specify the default DVMRP gateway for IP multicast traffic. Use the **no** form to remove the default gateway.

Syntax

default-gateway *ip-address*
no default-gateway

ip-address - IP address of the default DVMRP gateway.

Default Setting

None

Command Mode

Router Configuration

Command Usage

- The specified interface advertises itself as a default route to neighboring DVMRP routers. It advertises the default route out through its other interfaces. Neighboring routers on the other interfaces return Poison Reverse messages for the default route back to the router. When the router receives these messages, it records all the downstream routers for the default route.
- When multicast traffic with an unknown source address (i.e., not found in the route table) is received on the default upstream route interface, the router forwards this traffic out through the other interfaces (with known downstream routers). However, when multicast traffic with an unknown source address is received on another interface, the router drops it because only the default upstream interface can forward multicast traffic from an unknown source.

Example

```
Console(config-router)#default-gateway 10.1.0.253
Console(config-router)#
```


Downloaded from www.Manualslib.com manuals search engine

ip dvmrp

Use this command to enable DVMRP on the specified interface. Use the **no** form to disable DVMRP on this interface.

Syntax

ip dvmrp
no ip dvmrp

Default Setting

Disabled

Command Mode

Interface Configuration (VLAN)

Command Usage

To fully enable DVMRP, you need to enable multicast routing globally for the router with the **ip multicast-routing** command (page 3-187), enable DVMRP globally for the router with the **router dvmrp** command (page 3-191), and also enable DVMRP for each interface that will participate in multicast routing with the **ip dvmrp** command.

Example

```
Console(config)#interface vlan 1
Console(config-if)#ip dvmrp
Console(config-if)#end
Console#show ip dvmrp interface
Vlan 1 is up
  DVMRP is enabled
  Metric is 1

Console#
```


Downloaded from www.Manualslib.com manuals search engine

ip dvmrp metric

Use this command to configure the metric used in selecting the reverse path to networks connected directly to an interface on this router. Use the **no** form to restore the default value.

Syntax

ip dvmrp metric *interface-metric*
no ip dvmrp metric

interface-metric - Metric used to select the best reverse path. (Range: 1-31)

Default Setting

1

Command Mode

Interface Configuration (VLAN)

Command Usage

The DVMRP interface metric is used to choose the best reverse path when there are multiple paths to the same upstream destination. The lower cost path is the preferred path.

Example

```
Console(config)#interface vlan 1
Console(config-if)#ip dvmrp metric 2
Console(config-if)#
```

clear ip dvmrp route

Use this command to clear all dynamic routes learned by DVMRP.

Command Mode

Privileged Exec

Example

Downloaded from www.Manualslib.com manuals search engine

As shown below, this command clears everything from the route table except for the default route.

```
Console#clear ip dvmrp route
clear all ip dvmrp route
Console#show ip dvmrp route

    Source          Mask      Upstream_nbr   Interface Metric UpTime Expire
--------------- --------------- --------------- --------- ------ ------
------
      10.1.0.0   255.255.255.0     10.1.0.253     vlan1      1   1840      0
Console#
```

show router dvmrp

Use this command to display the global DVMRP configuration settings.

Command Mode

Normal Exec, Privileged Exec

Command Usage

This command displays the global DVMRP settings described in the preceding pages:

- Admin Status, router dvmrp, (page 3-191)
- Probe Interval (page 3-192)
- Nbr Expire (page 3-193)
- Minimum Flash Update Interval (page 3-194)
- Prune Lifetime (page 3-195)
- Route Report (page 3-194
- Default Gateway (page 3-196)
- Metric of Default Gateway (page 3-198)

Example

Downloaded from www.Manualslib.com manuals search engine

The default settings are shown in the following example:

```
Console#show route dvmrp
Admin Status                    : enable
Probe Interval                  : 10
Nbr expire                      : 35
Minimum Flash Update Interval   : 5
prune lifetime                  : 7200
route report                    : 60
Default Gateway                 : 0.0.0.0
Metric of Default Gateway       : 1
Console#
```

show ip dvmrp route

Use this command to display all entries in the DVMRP routing table.

Command Mode

Normal Exec, Privileged Exec

Example

DMVRP routes are shown in the following example:

```
Console#show ip dvmrp route

    Source          Mask      Upstream_nbr   Interface Metric UpTime Expire
--------------- --------------- --------------- --------- ------ ------
------
      10.1.0.0   255.255.255.0     10.1.0.253     vlan1      1  84438      0
      10.1.1.0   255.255.255.0     10.1.1.253     vlan2      1  84987      0
      10.1.8.0   255.255.255.0     10.1.0.254     vlan1      2  19729     97
Console#
```

Field	Description
Source	IP subnetwork that contains a multicast source, an upstream router, or an outgoing interface connected to multicast hosts.
Mask	Subnet mask that is used for the source address. This mask identifies the host address bits used for routing to specific subnets.
Upstream_nbr	The IP address of the network device immediately upstream for one or more multicast groups.
Interface	The IP interface on this router that connects to the upstream neighbor.
Metric	The metric for this interface used to calculate distance vectors.

Downloaded from www.Manualslib.com manuals search engine

Field	Description
UpTime	The time elapsed since this entry was created.
Expire	The time remaining before this entry will be aged out.

show ip dvmrp neighbor

Use this command to display all of the DVMRP neighbor routers.

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show ip dvmrp neighbor

     Address        Interface     Uptime   Expire   Capabilities
---------------- --------------- -------- -------- -------------
      10.1.0.254           vlan1    79315       32             6
Console#
```

Field	Description
Address	The IP address of the network device immediately upstream for this multicast delivery tree.
Interface	The IP interface on this router that connects to the upstream neighbor.
Uptime	The time since this device last became a DVMRP neighbor.
Expire	The time remaining before this entry will be aged out.
Capabilities	The neighboring router's capabilities may include: Leaf (bit 0) - Neighbor has only one interface with neighbors. Prune (bit 1) - Neighbor supports pruning. Generation ID (bit 2) - Neighbor sends its Generation ID in probe messages. Mtrace (bit 3) - Neighbor can handle multicast trace requests. SNMP (bit 4) - Neighbor is SNMP capable. Netmask - (bit 5) - Neighbor will accept network masks appended to the prune, graft, and graft acknowledgement messages. Reserved (bit 6 and 7) - Reserved for future use.

Downloaded from www.Manualslib.com manuals search engine

show ip dvmrp interface

Use this command to display the DVMRP configuration for interfaces which have enabled DVMRP.

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show ip dvmrp interface
Vlan 1 is up
  DVMRP is enabled
  Metric is 1

Console#
```

PIM-DM Multicast Routing Commands

Command	Function	Mode	Page
router pim	Enables PIM globally for the router	GC	3-203
ip pim dense-mode	Enables PIM on the specified interface	IC	3-204
ip pim hello-interval	Sets the interval between sending PIM hello messages	IC	3-205
ip pim hello-holdtime	Sets the time to wait for hello messages from a neighboring PIM router before declaring it dead	IC	3-206
ip pim trigger-hello-interval	Sets the maximum time before sending a triggered PIM Hello message	IC	3-206
ip pim join-prune-holdtime	Configures the hold time for the prune state	IC	3-207
ip pim graft-retry-interval	Configures the time to wait for a Graft acknowledgement before resending a Graft message	IC	3-208
ip pim max-graft-retries	Configures the maximum number of times to resend a Graft message if it has not been acknowledged	IC	3-209
show router pim	Displays the global PIM configuration settings	NE, PE	3-209

Downloaded from www.Manualslib.com manuals search engine

Command	Function	Mode	Page
show ip pim interface	Displays information about interfaces configured for PIM	NE, PE	3-210
show ip pim neighbor	Displays information about PIM neighbors	NE, PE	3-210

router pim

Use this command to enable Protocol-Independent Multicast - Dense Mode (PIM-DM) globally for the router and to enter router configuration mode. Use the **no** form to disable PIM-DM multicast routing.

Syntax

router pim
no router pim

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

This command enables PIM-DM globally for the router. You also need to enable PIM-DM for each interface that will support multicast routing using the **ip pim dense-mode** command (page 3-204), and make any changes necessary to the multicast protocol parameters.

Example

```
Console(config)#router pim
Console#show router pim
Admin Status: Enabled
Console#
```


Downloaded from www.Manualslib.com manuals search engine

ip pim dense-mode

Use this command to enable PIM-DM on the specified interface. Use the **no** form to disable PIM-DM on this interface.

Syntax

ip pim dense-mode
no pim dense-mode

Default Setting

Disabled

Command Mode

Interface Configuration (VLAN)

Command Usage

- To fully enable PIM-DM, you need to enable multicast routing globally for the router with the **ip multicast-routing** command (page 3-187), enable PIM-DM globally for the router with the **router pim** command (page 3-203), and also enable PIM-DM for each interface that will participate in multicast routing with the **ip pim dense-mode** command.
- If you enable PIM on an interface, you should also enable IGMP on that interface.
- Dense-mode interfaces are subject to multicast flooding by default, and are only removed from the multicast routing table when the router determines that there are no group members or downstream routers, or when a prune message is received from a downstream router.

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console(config)#interface vlan 1
Console(config-if)#ip pim dense-mode
Console#show ip pim interface
Vlan 1 is up
 PIM is enabled, mode is Dense.
 Internet address is 10.1.0.253.
 Hello time interval is 30 sec, trigger hello time interval is 5 sec.
 Hello holdtime is 105 sec.
 Join/Prune holdtime is 210 sec.
 Graft retry interval is 3 sec, max graft retries is 2.
 DR Internet address is 10.1.0.253, neighbor count is 0.

Console#
```

ip pim hello-interval

Use this command to configure the frequency at which PIM hello messages are transmitted. Use the **no** form to restore the default value.

Syntax

ip pim hello-interval *seconds*
no pim hello-interval

seconds - Interval between sending PIM hello messages. (Range: 1-65535)

Default Setting

30 seconds

Command Mode

Interface Configuration (VLAN)

Command Usage

Hello messages are sent to neighboring PIM routers from which this device has received probes, and are used to verify whether or not these neighbors are still active members of the multicast tree.

Example

```
Console(config-if)#ip pim hello-interval 60
Console(config-if)#
```


Downloaded from www.Manualslib.com manuals search engine

ip pim hello-holdtime

Use this command to configure the interval to wait for hello messages from a neighboring PIM router before declaring it dead. Use the **no** form to restore the default value.

Syntax

ip pim hello-holdtime *seconds*
no ip pim hello-interval

seconds - The hold time for PIM hello messages. (Range: 1-65535)

Default Setting

105 seconds

Command Mode

Interface Configuration (VLAN)

Command Usage

The **ip pim hello-holdtime** should be 3.5 times the value of **ip pim hello-interval** (page 3-205).

Example

```
Console(config-if)#ip pim hello-holdtime 210
Console(config-if)#
```

ip pim trigger-hello-interval

Use this command to configure the maximum time before transmitting a triggered PIM Hello message after the router is rebooted or PIM is enabled on an interface. Use the **no** form to restore the default value.

Syntax

ip pim triggerr-hello-interval *seconds*
no ip pim triggerr-hello-interval

seconds - The maximum time before sending a triggered PIM Hello message. (Range: 0-65535)

Downloaded from www.Manualslib.com manuals search engine

Default Setting

5 seconds

Command Mode

Interface Configuration (VLAN)

Command Usage

- When a router first starts or PIM is enabled on an interface, the hello-interval is set to random value between 0 and the trigger-hello-interval. This prevents synchronization of Hello messages on multi-access links if multiple routers are powered on simultaneously.
- Also, if a Hello message is received from a new neighbor, the receiving router will send its own Hello message after a random delay between 0 and the trigger-hello-interval.

Example

```
Console(config-if)#ip pim triggerr-hello-interval 10
Console(config-if)#
```

ip pim join-prune-holdtime

Use this command to configure of the hold time for the prune state. Use the **no** form to restore the default value.

Syntax

ip pim join-prune-holdtime *seconds*
no ip pim join-prune-holdtime

seconds - The hold time for the prune state. (Range: 0-65535)

Default Setting

210 seconds

Command Mode

Interface Configuration (VLAN)

Downloaded from www.Manualslib.com manuals search engine

Command Usage

The multicast interface that first receives a multicast stream from a particular source forwards this traffic to all other PIM interfaces on the router. If there are no requesting groups on that interface, the leaf node sends a prune message upstream and enters a prune state for this multicast stream. The prune state is maintained until the join-prune-holdtime timer expires or a graft message is received for the forwarding entry.

Example

```
Console(config-if)#ip pim join-prune-holdtime 60
Console(config-if)#
```

ip pim graft-retry-interval

Use this command to configure the time to wait for a Graft acknowledgement before resending a Graft. Use the **no** form to restore the default value.

Syntax

ip pim graft-retry-interval *seconds*
no ip pim graft-retry-interval

seconds - The time before resending a Graft. (Range: 0-65535)

Default Setting

3 seconds

Command Mode

Interface Configuration (VLAN)

Command Usage

A graft message is sent by a router to cancel a prune state. When a router receives a graft message, it must respond with an graft acknowledgement message. If this acknowledgement message is lost, the router that sent the graft message will resend it a number of times (as defined by the **ip pim max-graft-retries** command).

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console(config-if)#ip pim graft-retry-interval 9
Console(config-if)#
```

ip pim max-graft-retries

Use this command to configure the maximum number of times to resend a Graft message if it has not been acknowledged. Use the **no** form to restore the default value.

Syntax

ip pim max-graft-retries *retries*
no ip pim graft-retry-interval

retries - The maximum number of times to resend a Graft. (Range: 0-65535)

Default Setting

2

Command Mode

Interface Configuration (VLAN)

Example

```
Console(config-if)#ip pim max-graft-retries 5
Console(config-if)#
```

show router pim

Use this command to display the global PIM configuration settings.

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show router pim
Admin Status: Enabled
Console#
```


Downloaded from www.Manualslib.com manuals search engine

show ip pim interface

Use this command to display information about interfaces configured for PIM.

Syntax

show ip pim interface *vlan-id*

vlan-id - VLAN ID (Range: 1-4094)

Command Mode

Normal Exec, Privileged Exec

Command Usage

This command displays the PIM settings for the specified interface as described in the preceding pages. It also shows the address of the designated PIM router and the number of neighboring PIM routers.

Example

```
Console#show ip pim interface 1
Vlan 1 is up
 PIM is enabled, mode is Dense.
 Internet address is 10.1.0.253.
 Hello time interval is 30 sec, trigger hello time interval is 5 sec.
 Hello holdtime is 105 sec.
 Join/Prune holdtime is 210 sec.
 Graft retry interval is 3 sec, max graft retries is 2.
 DR Internet address is 10.1.0.254, neighbor count is 1.

Console#
```

show ip pim neighbor

Use this command to display information about PIM neighbors.

Syntax

show ip pim neighbor [*ip-address*]

ip-address - IP address of a PIM neighbor.

Default Setting

Displays information for all known PIM neighbors.

Downloaded from www.Manualslib.com manuals search engine

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show ip pim neighbor
    Address      VLAN Interface   Uptime   Expire   Mode
--------------- ---------------- -------- -------- -------
     10.1.0.254        1         17:38:16 00:01:25   Dense

Console#
```

Field	Description
Address	IP address of the next-hop router.
VLAN Interface	Interface number that is attached to this neighbor.
Uptime	The duration this entry has been active.
Expire	The time before this entry will be removed.
Mode	PIM mode used on this interface. (Only Dense Mode is supported.)

Router Redundancy Commands

Router redundancy protocols use a virtual IP address to support a primary router and multiple backup routers. The backup routers can be configured to take over the workload if the master router fails, or can also be configured to share the traffic load. The primary goal of router redundancy is to allow a host device which has been configured with a fixed gateway to maintain network connectivity in case the primary gateway goes down.

Command Groups	Function	Page
Virtual Router Redundancy Protocol	Configures interface settings for VRRP	3-212
Hot Standby Router Protocol	Configures interface settings for HSRP	3-225

Downloaded from www.Manualslib.com manuals search engine

Virtual Router Redundancy Protocol Commands

To configure VRRP, select an interface on one router in the group to serve as the master virtual router. This physical interface is used as the virtual address for the router group. Now set the same virtual address and a priority on the backup routers, and configure an authentication string. You can also enable the preempt feature which allows a router to take over as the master router when it comes on line.

Command	Function	Mode	Page
vrrp ip	Enables VRRP and sets the IP address of the virtual router	IC	3-212
vrrp authentication key	Configures a key used to authenticate VRRP packets received from other routers	IC	3-214
vrrp priority	Sets the priority of this router in the VRRP group	IC	3-215
vrrp timers advertise	Sets the interval between successive advertisements by the master virtual router	IC	3-216
vrrp preempt	Configures the router to take over as master virtual router for a VRRP group if it has a higher priority than the current master virtual router	IC	3-217
show vrrp	Displays VRRP status information	PE	3-218
show vrrp interface	Displays VRRP status information for the specified interface	PE	3-220
show vrrp router counters	Displays VRRP statistics	PE	3-222
show vrrp interface counters	Displays VRRP statistics for the specified interface	PE	3-222
clear vrrp router counters	Clears VRRP router statistics	PE	3-223
clear vrrp interface counters	Clears VRRP interface statistics	PE	3-223

vrrp ip

Use this command to enable the Virtual Router Redundancy Protocol (VRRP) on an interface and specify the IP address of the virtual router.

Downloaded from www.Manualslib.com manuals search engine

Use the **no** form to disable VRRP on an interface and remove the IP address from the virtual router.

Syntax

vrrp *group* **ip** *ip-address* [**secondary**]
no vrrp *group* **ip** *ip-address* [**secondary**]

- *group* - Identifies the virtual router group. (Range: 1-255)
- *ip-address* - The IP address of the virtual router.
- **secondary** - Specifies additional secondary IP addresses assigned to the current VLAN interface that are supported by this VRRP group.

Default Setting

No virtual router groups are configured.

Command Mode

Interface (VLAN)

Command Usage

- The interfaces of all routers participating in a virtual router group must be within the same IP subnet.
- The IP address assigned to the virtual router must already be configured on the router that will be the Owner. In other words, the IP address specified in this command must already exist on one, and only one, router in the virtual router group, and the network mask for the virtual router address is derived from the Owner. The Owner will also assume the role of the Master virtual router in the group.
- If you have multiple secondary addresses configured on the current VLAN interface, you can use this command with the **secondary** keyword to add any secondary address that will be supported by the virtual router.
- VRRP is enabled as soon as this command is entered. If you need to customize any of the other parameters for VRRP such as authentication, priority, or advertisement interval, then first configure these parameters before enabling VRRP.

Example

Downloaded from www.Manualslib.com manuals search engine

This example creates VRRP group 1 using the primary interface for VLAN 1 as the VRRP group Owner, and also adds a secondary interface as a member of the group.

```
Console(config)#interface vlan 1
Console(config-if)#vrrp 1 ip 192.168.1.6
Console(config-if)#vrrp 1 ip 192.168.2.6 secondary
Console(config-if)#
```

vrrp authentication

Use this command to specify the key used to authenticate VRRP packets received from other routers. Use the **no** form to prevent authentication.

Syntax

vrrp *group* **authentication** *key*
no vrrp *group* **authentication**

- *group* - Identifies the virtual router group. (Range: 1-255)
- *key* - Authentication string. (Range: 1-8 alphanumeric characters)

Default Setting

No key is defined.

Command Mode

Interface (VLAN)

Command Usage

- All routers in the same VRRP group must be configured with the same authentication key.
- When a VRRP packet is received from another router in the group, its authentication key is compared to the string configured on this router. If the keys match, the message is accepted. Otherwise, the packet is discarded.
- Plain text authentication does not provide any real security. It is supported only to prevent a misconfigured router from participating in VRRP.

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console(config-if)#vrrp 1 authentication bluebird
Console(config-if)#
```

vrrp priority

Use this command to set the priority of this router in a VRRP group. Use the **no** form to restore the default setting.

Syntax

vrrp *group* **priority** *level*
no vrrp *group* **priority**

- *group* - Identifies the VRRP group. (Range: 1-255)
- *level* - Priority of this router in the VRRP group. (Range: 1-254)

Default Setting

100

Command Mode

Interface (VLAN)

Command Usage

- A router that has a physical interface with the same IP address as that used for the virtual router will become the master virtual router. The backup router with the highest priority will become the master router if the current master fails. When the original master router recovers, it will take over as the active master router again.
- If two or more routers are configured with the same VRRP priority, the router with the higher IP address is elected as the new master router if the current master fails.
- If the backup preempt function is enabled with the **vrrp preempt** command, and a backup router with a priority higher than the current acting master comes on line, this backup router will take over as the new acting master. However, note that if the original master (i.e., the owner of the VRRP IP address) comes back on line, it will always resume control as the master.

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console(config-if)#vrrp 1 priority 1
Console(config-if)#
```

Related Commands

vrrp preempt (3-217)

vrrp timers advertise

Use this command to set the interval at which the master virtual router sends advertisements communicating its state as the master. Use the **no** form to restore the default interval.

Syntax

vrrp *group* **timers advertise** *interval*
no vrrp *group* **timers advertise**

- *group* - Identifies the VRRP group. (Range: 1-255)
- *interval* - Advertisement interval for the master virtual router. (Range: 1-255 seconds)

Default Setting

1 second

Command Mode

Interface (VLAN)

Command Usage

- VRRP advertisements from the current master virtual router include information about its priority and current state as the master.
- VRRP advertisements are sent to the multicast address 224.0.0.8. Using a multicast address reduces the amount of traffic that has to processed by network devices that are not part of the designated VRRP group.
- If the master router stops sending advertisements, backup routers will bid to become the master router based on priority. The dead interval

Downloaded from www.Manualslib.com manuals search engine

before attempting to take over as the master is three times the hello interval plus half a second

Example

```
Console(config-if)#vrrp 1 timers advertise 5
Console(config-if)#
```

vrrp preempt

Use this command to configure the router to take over as the master virtual router for a VRRP group if it has a higher priority than the current acting master router. Use the **no** form to disable preemption.

Syntax

vrrp *group* **preempt** [**delay** *seconds*]
no vrrp *group* **preempt**

- *group* - Identifies the VRRP group. (Range: 1-255)
- *seconds* - The time to wait before issuing a claim to become the master. (Range: 0-120 seconds)

Default Setting

Preempt: Enabled
Delay: 0 seconds

Command Mode

Interface (VLAN)

Command Usage

- If preempt is enabled, and this backup router has a priority higher than the current acting master, it will take over as the new master. However, note that if the original master (i.e., the owner of the VRRP IP address) comes back on line, it will always resume control as the master.
- The delay can give additional time to receive an advertisement message from the current master before taking control. If the router attempting to become the master has just come on line, this delay also gives it time to gather information for its routing table before actually preempting the currently active router.

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console(config-if)#vrrp 1 preempt delay 10
Console(config-if)#
```

Related Commands

vrrp priority (3-215)

show vrrp

Use this command to display status information for VRRP.

Syntax

show vrrp [**brief** | *group*]

- **brief** - Displays summary information for all VRRP groups on this router.
- *group* - Identifies a VRRP group. (Range: 1-255)

Defaults

None

Command Mode

Privileged Exec

Command Usage

- Use this command without any keywords to display the full listing of status information for all VRRP groups configured on this router.
- Use this command with the **brief** keyword to display a summary of status information for all VRRP groups configured on this router.
- Specify a group number to display status information for a specific group

Example

Downloaded from www.Manualslib.com manuals search engine

This example displays the full listing of status information for all groups.

```
Console#show vrrp
 Vlan 1 - Group 1,
 state                              Master
 Virtual IP address                 192.168.1.6
 Virtual MAC address                00-00-5E-00-01-01
 Advertisement interval             5 sec
 Preemption                         enabled
 Min delay                          10 sec
 Priority                           1
 Authentication                     SimpleText
 Authentication key                 bluebird
 Master Router                      192.168.1.6
 Master priority                    255
 Master Advertisement interval      5 sec
 Master down interval               15
Console#
```

Field	Description
State	VRRP role of this interface (master or backup)
Virtual IP address	Virtual address that identifies this VRRP group
Virtual MAC address	Virtual MAC address derived from the owner of the virtual IP address
Advertisement interval	Interval at which the master virtual router advertises its role as the master
Preemption	Shows whether or not a higher priority router can preempt the current acting master
Min delay	Delay before a router with a higher priority can preempt the current acting master
Priority	Priority of this router
Authentication	Authentication mode used to verify VRRP packets
Authentication key	Key used to authenticate VRRP packets received from other routers
Master Router	IP address of the router currently acting as the VRRP group master
Master priority	The priority of the router currently acting as the VRRP group master

Downloaded from www.Manualslib.com manuals search engine

Field	Description
Master Advertisement interval	The advertisement interval configured on the VRRP master.
Master down interval	The down interval configured on the VRRP master (This interval is used by all the routers in the group regardless of their local settings)

This example displays the brief listing of status information for all groups.

```
Console#show vrrp brief
Interface   Grp    State    Virtual addr     Int   Pre   Prio
-------------------------------------------------------------
vlan 1      1      Master   192.168.1.6      5      E    1
Console#
```

Field	Description
Interface	VLAN interface
Grp	VRRP group
State	VRRP role of this interface (master or backup)
Virtual addr	Virtual address that identifies this VRRP group
Int	Interval at which the master virtual router advertises its role as the master
Pre	Shows whether or not a higher priority router can preempt the current acting master
Prio	Priority of this router

show vrrp interface

Use this command to display status information for the specified VRRP interface.

Syntax

show vrrp interface vlan *vlan-id* [**brief**]

- *vlan-id* - Identifier of configured VLAN interface. (Range: 1-4094)
- **brief** - Displays summary information for all VRRP groups on this router.

Downloaded from www.Manualslib.com manuals search engine

Defaults

None

Command Mode

Privileged Exec

Example

This example displays the full listing of status information for VLAN 1.

```
Console#show vrrp interface vlan 1
 Vlan 1 - Group 1,
 state                            Master
 Virtual IP address               192.168.1.6
 Virtual MAC address              00-00-5E-00-01-01
 Advertisement interval           5 sec
 Preemption                       enabled
 Min delay                        10 sec
 Priority                         1
 Authentication                   SimpleText
 Authentication key               bluebird
 Master Router                    192.168.1.6
 Master priority                  1
 Master Advertisement interval    5 sec
 Master down interval             15
Console#
```

* Refer to “show vrrp” on page 3-218 for a description of the display items.

Downloaded from www.Manualslib.com manuals search engine

show vrrp router counters

Use this command to display counters for errors found in VRRP protocol packets.

Command Mode

Privileged Exec

Example

Note that unknown errors indicate VRRP packets received with an unknown or unsupported version number.

```
Console#show vrrp router counters
 Total Number of VRRP Packets with Invalid Checksum : 0
 Total Number of VRRP Packets with Unknown Error    : 0
 Total Number of VRRP Packets with Invalid VRID     : 0
Console#
```

show vrrp interface counters

Use this command to display counters for VRRP protocol events and errors that have occurred for the specified group and interface.

show vrrp *group* **interface vlan** *interface* **counters**

- *group* - Identifies a VRRP group. (Range: 1-255)
- *interface* - Identifier of configured VLAN interface. (Range: 1-4094)

Defaults

None

Command Mode

Privileged Exec

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console#show vrrp 1 interface vlan 1 counters
 Total Number of Times Transitioned to MASTER                        : 6
 Total Number of Received Advertisements Packets                     : 0
 Total Number of Received Error Advertisement Interval Packets       : 0
 Total Number of Received Authentication Failures Packets            : 0
 Total Number of Received Error IP TTL VRRP Packets                  : 0
 Total Number of Received Priority 0 VRRP Packets                    : 0
 Total Number of Sent Priority 0 VRRP Packets                        : 5
 Total Number of Received Invalid Type VRRP Packets                  : 0
 Total Number of Received Error Address List VRRP Packets            : 0
 Total Number of Received Invalid Authentication Type VRRP Packets   : 0
 Total Number of Received Mismatch Authentication Type VRRP Packets  : 0
 Total Number of Received Error Packet Length VRRP Packets           : 0
Console#
```

* Refer to “Displaying VRRP Group Statistics” on page 3-235 for a description of the display items.

clear vrrp router counters

Use this command to clear VRRP system statistics.

Command Mode

Privileged Exec

Example

```
Console#clear vrrp router counters
Console#
```

clear vrrp interface counters

Use this command to clear VRRP system statistics for the specified group and interface.

clear vrrp *group* **interface** *interface* **counters**

- *group* - Identifies a VRRP group. (Range: 1-255)
- *interface* - Identifier of configured VLAN interface. (Range: 1-4094)

Defaults

None

Downloaded from www.Manualslib.com manuals search engine

Command Mode

Privileged Exec

Example

```
Console#clear vrrp 1 interface 1 counters
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Hot Standby Router Protocol Commands

To configure HSRP, add the interface for each router that will participate in the virtual router group, set the priorities, and configure an authentication string. The HSRP protocol will automatically select the master and standby router based on the priority settings. You can also enable the preempt feature which allows a router to take over as the master router when it comes on line. HSRP also allows you to specify a set of interfaces that dynamically change the router priority based on their availability.

Command	Function	Mode	Page
standby ip	Enables HSRP	IC	3-225
standby priority	Sets the priority of this router in the HSRP group	IC	3-227
standby preempt	Configures the router to take over as master virtual router for an HSRP group if it has a higher priority than the current master virtual router	IC	3-228
standby authentication	Configures a key used to authenticate HSRP packets received from other routers	IC	3-230
standby timers	Sets the time between the master and standby router sending hello packets, and the time before other routers declare the active master router or standby router down	IC	3-231
standby track	Configures an interface so that the HSRP priority changes based on the availability of other interfaces on this router	IC	3-232
show standby	Displays HSRP status information	PE	3-234
show standby interface	Displays HSRP status information for the specified interface	PE	3-237

standby ip

Use this command to enable the Hot Standby Router Protocol (HSRP) on an interface and specify the IP address of the virtual router. Use the **no**

Downloaded from www.Manualslib.com manuals search engine

form to disable HSRP on an interface and remove the IP address for the virtual router.

Syntax

standby [*group*] **ip** [*ip-address* [**secondary**]]
no standby [*group*] **ip** [*ip-address*]

- *group* - Identifies the virtual router group. (Range: 0-255)
- *ip-address* - The designated IP address of the virtual router.
- **secondary** - Specifies additional IP addresses supported by this group.

Default Setting

Group number: 0
Virtual router groups: none configured

Command Mode

Interface (VLAN)

Command Usage

- The designated IP address must be configured on at least one router in the virtual router group. If an IP address is specified in this command, that address is used as the designated address for the virtual group. If an IP address is not specified, the designated address is learned through the exchange of HSRP messages. Note that the designated address cannot be the same as a physical address.
- The subnet mask for the physical interface on which the designated address is configured is used as the subnet mask of the designated address. The interfaces of all routers participating in a virtual router group must be within the same IP subnet.
- Configuring a new designated address on the current master router will override the designated address currently is use.
- If you have multiple secondary addresses configured on the current VLAN interface, you can use this command with the **secondary** keyword to add any secondary address that will be supported by the virtual router.

Downloaded from www.Manualslib.com manuals search engine

- HSRP is enabled once the designated address and priority are configured, and the master and standby routers are elected based on highest priority. If you need to customize any of the other parameters for HSRP such as authentication, tracking, or advertisement interval, then first configure these parameters before enabling HSRP.

Example

This example creates HSRP group 1 for VLAN 1, and also adds a secondary interface as a member of the group.

```
Console(config)#interface vlan 1
Console(config-if)#standby 1 ip 192.168.1.7
Console(config-if)#standby 1 ip 192.168.2.6 secondary
Console(config-if)#
```

standby priority

Use this command to set the priority of this router in a HSRP group. Use the **no** form to restore the default setting.

Syntax

standby [*group*] **priority** *level*
no standby [*group*] **priority**

- *group* - Identifies the HSRP group. (Range: 0-255)
- *level* - Priority of this router in the HSRP group. (Range: 1-255)

Default Setting

Group number: 0
Priority: 100

Command Mode

Interface (VLAN)

Command Usage

- The router with the highest priority is elected as the master virtual router. The router with the next highest priority is elected as the standby router. The standby router will become the master router if the current master fails. When the original master router recovers, it will

Downloaded from www.Manualslib.com manuals search engine

become the active master router again if the configured priorities have not been changed.

- If two or more routers are configured with the same HSRP priority, the router with the higher IP address is elected as the new master router if the current master fails.
- The priority setting takes precedence over authentication. In other words, if a router with a higher priority than any other router comes on line, but is not configured with the **standby authentication** command, or is configured with the wrong string, it will still take over as the active master.
- The HSRP priority can change dynamically if an interface is configured with the **standby track** command and another interface on the router fails or comes back on line.

Example

```
Console(config-if)#standby 1 priority 10
Console(config-if)#
```

Related Commands

standby authentication (3-230)
standby track (3-232)

standby preempt

Use this command to configure the router to take over as the master virtual router for an HSRP group if it has higher priority than the current master virtual router. Use the **no** form to disable preemption.

Syntax

standby [*group*] **preempt** [**delay** *seconds*]
no standby [*group*] **preempt** [**delay**]

- *group* - Identifies the HSRP group. (Range: 0-255)
- *seconds* - The time to wait before issuing a claim to become the master. (Range: 0-3600 seconds)

Downloaded from www.Manualslib.com manuals search engine

Default Setting

Group number: 0
Preempt: Disabled
Delay: 0 seconds

Command Mode

Interface (VLAN)

Command Usage

- If preempt is enabled, and this router has a priority higher than the current acting master, it will take over as the new master. If preempt is not enabled, this router will only take over if it has the highest priority in the group and the current master stops sending hello messages or sends other messages indicating that it is no longer acting as the designated router.
- The delay can give additional time to receive an advertisement message from the current master before taking control. If the router attempting to become the master has just come on line, this delay also gives it time to gather information for its routing table before actually preempting the currently active router.

Example

```
Console(config-if)#standby 1 preempt delay 10
Console(config-if)#
```

Related Commands

standby priority (3-227)

Downloaded from www.Manualslib.com manuals search engine

standby authentication

Use this command to specify the key used to authenticate HSRP packets received from other routers. Use the **no** form to delete an authentication string.

Syntax

standby [*group*] **authentication** *string*
no standby [*group*] **authentication**

- *group* - Identifies the HSRP group. (Range: 0-255)
- *string* - Authentication string. (Range: 1-8 alphanumeric characters)

Default Setting

Group number: 0
String: not defined

Command Mode

Interface (VLAN)

Command Usage

- All routers in the same HSRP group must be configured with the same authentication string. The authentication string is sent unencrypted in all HSRP messages.
- When an HSRP packet is received from another router in the group, its authentication string is compared to the string configured on this router. If the strings match, the message is accepted. Otherwise, the packet is discarded. If the authentication strings do not match, this router will not be able to learn the designated address for the group and timer values from other routers. However, even if authentication fails, this cannot prevent a router from taking over as the master router if it has the highest priority in the group.
- Priority takes precedence over authentication. In other words, if a router is configured with the **standby priority** command to have the highest priority in the group, but does not have an authentication string, or is configured with the wrong string, it will still take over as the active master.

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console(config-if)#standby 1 authentication bluebird
Console(config-if)#
```

Related Commands

standby priority (3-227)

standby timers

Use this command to set the time between the master and standby router sending hello packets, and the time before other routers declare the active master router or standby router down. Use the **no** form to restore the default timer values.

Syntax

standby [*group*] **timers** *hellotime holdtime*
no standby [*group*] **timers**

- *group* - Identifies the HSRP group. (Range: 0-255)
- *hellotime* - Advertisement interval for the master and standby virtual router. (Range: 1-254 seconds)
- *holdtime* - Time before the master or standby router is declared down. (Range: hellotime+1 to 255 seconds)

Default Setting

Group number: 0
Hellotime: 3 seconds
Holdtime: 10 seconds

Command Mode

Interface (VLAN)

Command Usage

- HSRP advertisements from the master and standby virtual router include information about their priority, timer values, and current state as the master or standby router.

Downloaded from www.Manualslib.com manuals search engine

- Routers on which the timer settings have not been configured can learn the current timer values from the master or standby router. Timers configured on the master router always override any other timer settings. All routers in an HSRP group should be configured with the same timer values.
- If the master router stops sending advertisements, backup routers will bid to become the master based on priority. The hold time before declaring a router dead should be normally be set to a value 3 times or more than the hello time.
- HSRP advertisements are sent to the multicast address 224.0.0.2. Using a multicast address reduces the amount of traffic that has to processed by network devices that are not part of the designated HSRP group.

Example

This example sets the timers for group 1 to 6 seconds for the hello time, and 18 seconds for the hold time.

```
Console(config-if)#standby 1 timers 6 18
Console(config-if)#
```

standby track

Use this command to configure an interface so that the HSRP priority changes based on the availability of other IP interfaces on this router. Use the **no** form to disable tracking.

Syntax

standby [*group*] **track vlan** *vlan-id* [*interface-priority*]
no standby [*group*] **track vlan** *vlan-id*

- *group* - Identifies the HSRP group. (Range: 0-255)
- *vlan-id* - VLAN configured with an IP address. (Range: 1-4094)
- *interface-priority* - Amount by which the HSRP router priority is decremented (or incremented) when the interface goes down (or comes back up). (Range: 1-255)

Downloaded from www.Manualslib.com manuals search engine

Default Setting

Group number: 0
Interface priority: 10

Command Mode

Interface (VLAN)

Command Usage

- This command adjusts the HSRP router priority based on the availability of its IP interfaces. When a tracked interface goes down, the HSRP router priority decreases by the specified value, and increases by the same value when it comes back up. You can specify up to 32 interfaces to be tracked.
- If you specify a VLAN interface that has not been configured with an IP address, this command will not affect the HSRP router priority.
- If you configure multiple tracked interfaces, and also set the interface priority, the effect on HSRP router priority is cumulative when one or more interfaces go up or down. However, if you configure multiple tracked interfaces, but do not set the interface priority, HSRP router priority will only be changed by the default interface priority value of 10; i.e., the effect is not cumulative.

Example

This example tracks the VLAN 2 IP interface, and sets the amount by which to adjust the HSRP router priority on the VLAN 1 interface to 5.

```
Console(config)interface vlan 1
Console(config-if)#standby 1 track vlan 2 5
Console(config-if)#
```


Downloaded from www.Manualslib.com manuals search engine

show standby

Use this command to display status information for HSRP.

Syntax

show standby [**active** | **init** | **listen** | **standby**] [**brief**]

- **active** - Displays HSRP groups in the active state.
- **init** - Displays HSRP groups in the initial state.
- **listen** - Displays HSRP groups in the listen or learn state.
- **standby** - Displays HSRP groups in the standby or speak state.
- **brief** - Displays summary information for all HSRP groups on this router.

Defaults

Displays detailed information for each group.

Command Mode

Privileged Exec

Example

This example displays the full listing of status information for all groups.

```
Console#show standby
Vlan 1 - Group 1
Local State is Active, priority 5 (confgd 10), may preempt
Preemption delayed for 10 secs
Hellotime 6 sec, holdtime 18 sec
Next hello sent in 0: 0: 5
Host standby IP address is 192.168.1.7 configured
Active router is local
Standby router is unknown
Standby virtual mac address is  0- 0- C- 7-AC- 1
Authentication text "bluebird"
Tracking interface states for 1 interfaces, 0 up
   Down    Vlan2     5
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Field	Description
Local state	State of the local router: • Active - Current master router. • Standby - Designated backup router next in line to take over as the master router. • Speak - Router is sending packets to claim the master or standby role. • Init - Router is not ready to participate in HSRP. A router may be in this state because the associated interface is not up, the interface is in an HSRP group on other routers in the network that were learned via snooping, or a local group has been configured without a specified IP interface. • Listen - Router is not in the active nor standby state. If no messages are received from the active or standby router, it will start to speak. • Learn - Router is not in the active nor standby state, nor does it have enough information to attempt to claim the master or standby roles.
priority	Priority of this router.
may preempt	Router will attempt to take over as the master router if its priority is higher.
Preemption delayed	Delay before a router with higher priority can preempt the current acting master
Hellotime	Interval at which this router advertises when acting as the master or standby router
Next hello sent	Time before the next hello packet will be sent
Host standby IP address	IP address of the master router
Active router	The master router can be "local" or an IP address. Local implies this router. If an address is display, it indicates the current active master router.
Standby router	The standby router can be "local" or an IP address. Local implies this router. If an address is display, it indicates the current standby router.
Standby virtual mac address	The virtual MAC address for this HSRP group. This is always 0000.0C07.ACxy, where xy is the hexadecimal value of the group number.

Downloaded from www.Manualslib.com manuals search engine

Field	Description
Authentication text	Key used to authenticate HSRP packets received from other routers.
Tracking interface states	List of interfaces that are being tracked and their corresponding states.

This example displays the brief listing of status information for all groups.

```
Console#show vrrp brief
Interface Grp Prio P State    Active addr    Standby addr      Group addr
-------------------------------------------------------------------------
Vlan1       1    5 T  Active        Local         0.0.0.0     192.168.1.7
Console#
```

Field	Description
Interface	VLAN interface
Grp	HSRP group
Prio	Priority of this router
P	Shows whether or not a higher priority router can preempt the current acting master
State	Local state as described in the preceeding table
Active addr	Address of the master router
Standby addr	Address of the standby router
Group addr	Address of the HSRP group

Downloaded from www.Manualslib.com manuals search engine

show standby interface

Use this command to display HSRP status information for the specified interface.

Syntax

show standby interface vlan *vlan-id* [**group** *group*] [**active** | **init** | **listen** | **standby**] [**brief**]

- *vlan-id* - Identifier of configured VLAN interface. (Range: 1-4094)
- *group* - Identifies the HSRP group. (Range: 0-255)
- **active** - Displays HSRP groups in the active state.
- **init** - Displays HSRP groups in the initial state.
- **listen** - Displays HSRP groups in the listen or learn state.
- **standby** - Displays HSRP groups in the standby or speak state.
- **brief** - Displays summary information for all HSRP groups on this router.

Defaults

Displays detailed information for each group.

Command Mode

Privileged Exec

Downloaded from www.Manualslib.com manuals search engine

Example

This example displays the full listing of status information for VLAN 1.

```
Console#show standby interface vlan 1 group 1
Vlan 1 - Group 1
Local State is Active, priority 5 (confgd 10), may preempt
Preemption delayed for 10 secs
Hellotime 6 sec, holdtime 18 sec
Next hello sent in 0: 0: 0
Host standby IP address is 192.168.1.7 configured
Active router is local
Standby router is unknown
Standby virtual mac address is  0- 0- C- 7-AC- 1
Authentication text "bluebird"
Tracking interface states for 1 interfaces, 0 up
   Down    Vlan2     5
Console#show standby interface vlan 1 group 1 brief
Interface Grp Prio P State    Active addr    Standby addr      Group addr
---------------------------------------------------------------------------
Vlan1       1    5 T  Active        Local         0.0.0.0     192.168.1.7
Console#
```

For a description of the displayed information, see the preeeding “show standby” command.

Downloaded from www.Manualslib.com manuals search engine

Appendix A
Software Specifications

Software Features

Authentication
  Local, RADIUS, TACACS, Port (802.1x), HTTPS, SSH, Port Security

Access Control Lists
  IP, MAC (up to 32 lists)

DHCP Client, Relay, Server

DNS Server

Port Configuration
  1000BASE-T: 10/100/1000 Mbps, half/full duplex
  1000BASE-SX/LX: 1000 Mbps, full duplex

Flow Control
  Full Duplex: IEEE 802.3x
  Half Duplex: Back pressure

Broadcast Storm Control
  Traffic throttled above a critical threshold

Port Mirroring
  Multiple source ports, one destination port

Rate Limits
  Input Limit
  Output limit
  Range (configured per port)

Port Trunking
  Static trunks (Cisco EtherChannel compliant)
  Dynamic trunks (Link Aggregation Control Protocol)

Spanning Tree Protocol
  Spanning Tree Protocol (STP, IEEE 802.1D)

Downloaded from www.Manualslib.com manuals search engine

Rapid Spanning Tree Protocol (RSTP, IEEE 802.1w)
Multiple Spanning Tree Protocol (MSTP, IEEE 802.1s)

VLAN Support
Up to 255 groups; port-based, protocol-based, or tagged (802.1Q),
GVRP for automatic VLAN learning, private VLANs

Class of Service
Supports eight levels of priority and Weighted Round Robin Queueing
(which can be configured by VLAN tag or port),
Layer 3/4 priority mapping: IP Port, IP Precedence, IP DSCP

Multicast Filtering
IGMP Snooping (Layer 2)
IGMP (Layer 3)

Multicast Routing
DVMRP, PIM-DM

IP Routing
ARP, Proxy ARP
Static routes
RIP, RIPv2 and OSPFv2 dynamic routing
VRRP (Virtual Router Redundancy Protocol)
HSRP (Hot Standby Router Protocol)

Additional Features
BOOTP client
CIDR (Classless Inter-Domain Routing)
SNTP (Simple Network Time Protocol)
SNMP (Simple Network Management Protocol)
RMON (Remote Monitoring, groups 1,2,3,9)
SMTP Email Alerts

Management Features

In-Band Management
Telnet, web-based HTTP or HTTPS, SNMP manager, or Secure Shell

Out-of-Band Management
RS-232 DB-9 console port

Software Loading
TFTP in-band or XModem out-of-band

Downloaded from www.Manualslib.com manuals search engine

SNMP
  Management access via MIB database
  Trap management to specified hosts

RMON
  Groups 1, 2, 3, 9 (Statistics, History, Alarm, Event)

Standards

IEEE 802.3 Ethernet,
IEEE 802.3u Fast Ethernet
IEEE 802.3x Full-duplex flow control (ISO/IEC 8802-3)
IEEE 802.3z Gigabit Ethernet,
IEEE 802.3ab 1000BASE-T
IEEE 802.3ac VLAN tagging
IEEE 802.1Q VLAN
IEEE 802.1v Protocol-based VLANs
IEEE 802.3ad Link Aggregation Control Protocol
IEEE 802.1D Spanning Tree Protocol and traffic priorities
IEEE 802.1p Priority tags
IEEE 802.1s Multiple Spanning Tree Protocol
IEEE 802.1w Rapid Spanning Tree Protocol
IEEE 802.1x Port Authentication
ARP (RFC 826)
DHCP (RFC 1541)
DVMRP (RFC 1075)
HSRP (RFC 2281)
HTTPS
ICMP (RFC 792)
IGMP (RFC 1112)
IGMPv2 (RFC 2236)
OSPF (RFC 2328, 1587)
PIM-DM (draft-ietf-idmr-pim-dm-06)
RADIUS+ (RFC 2618)
RIP (RFC 1058)
RIPv2 (RFC 2453)
RMON (RFC 1757 groups 1,2,3,9)
SNMP (RFC 1157)
SNMPv2 (RFC 1907)

Downloaded from www.Manualslib.com manuals search engine

SNTP (RFC 2030)
SSH (Version 2.0)
VRRP (RFC 2338)

Management Information Bases

Bridge MIB (RFC 1493)
DVMRP MIB
Entity MIB (RFC 2737)
Ethernet MIB (RFC 2665)
Ether-like MIB (RFC 2665)
Extended Bridge MIB (RFC 2674)
Extensible SNMP Agents MIB (RFC 2742)
Forwarding Table MIB (RFC 2096)
IGMP MIB (RFC 2933)
Interface Group MIB (RFC 2233)
Interfaces Evolution MIB (RFC 2863)
IP MIB (RFC 2011)
IP Multicasting related MIBs
MAU MIB (RFC 2668)
MIB II (RFC 1213)
OSPF MIB (RFC 1850)
PIM MIB (RFC 2934)
Port Access Entity MIB (IEEE 802.1x)
Private MIB
Quality of Service MIB
RADIUS Authentication Client MIB (RFC 2621)
RIP1 MIB (RFC 1058)
RIP2 MIB (RFC 2453)
RMON MIB (RFC 2819)
RMON II Probe Configuration Group (RFC 2021, partial implementation)
SNMP framework MIB (RFC 2571)
SNMP-MPD MIB (RFC 2572)
SNMP Target MIB, SNMP Notification MIB (RFC 2573)
SNMP User-Based SM MIB (RFC 2574)
SNMP View Based ACM MIB (RFC 2575)
SNMP Community MIB (RFC 2576)
TACACS+ Authentication Client MIB

Downloaded from www.Manualslib.com manuals search engine

TCP MIB (RFC 2013)
Trap (RFC 1215)
UDP MIB (RFC 2012)
VRRP MIB (RFC 2787)

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

APPENDIX B
TROUBLESHOOTING

Troubleshooting Chart	
Symptom	**Action**
Cannot connect using Telnet, web browser, or SNMP software	• Be sure you have configured the VLAN interface through which the management station is connected with a valid IP address, subnet mask and default gateway. • If you are trying to connect to the switch via the IP address for a tagged VLAN group, your management station must include the appropriate tag in its transmitted frames. • Check that you have a valid network connection to the switch and that the port you are using has not been disabled. • Check network cabling between the management station and the switch. • If you cannot connect using Telnet or SSH, you may have exceeded the maximum number of concurrent Telnet/SSH sessions permitted. Try connecting again at a later time.
Cannot access the on-board configuration program via a serial port connection	• Be sure you have set the terminal emulator program to VT100 compatible, 8 data bits, 1 stop bit, no parity, and the baud rate set to any of the following (9600, 19200, 38400, 57600, 115200 bps). • Check that the null-modem serial cable conforms to the pin-out connections provided in the Installation Guide.
Forgot or lost the password	• Contact your local distributor.

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

GLOSSARY

Access Control List (ACL)

ACLs can limit network traffic and restrict access to certain users or devices by checking each packet for certain IP or MAC (i.e., Layer 2) information.

Address Resolution Protocol (ARP)

ARP converts between IP addresses and MAC (i.e., hardware) addresses. ARP is used to locate the MAC address corresponding to a given IP address. This allows the switch to use IP addresses for routing decisions and the corresponding MAC addresses to forward packets from one hop to the next.

Boot Protocol (BOOTP)

BOOTP is used to provide bootup information for network devices, including IP address information, the address of the TFTP server that contains the devices system files, and the name of the boot file.

Class of Service (CoS)

CoS is supported by prioritizing packets based on the required level of service, and then placing them in the appropriate output queue. Data is transmitted from the queues using weighted round-robin service to enforce priority service and prevent blockage of lower-level queues. Priority may be set according to the port default, the packet's priority bit (in the VLAN tag), TCP/UDP port number, IP Precedence bit, or DSCP priority bit.

Differentiated Services Code Point Service (DSCP)

DSCP uses a six-bit tag to provide for up to 64 different forwarding behaviors. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding. The DSCP bits are mapped to the Class of Service categories, and then into the output queues.

Domain Name Service (DNS)

A system used for translating host names for network nodes into IP addresses.

Downloaded from www.Manualslib.com manuals search engine

Distance Vector Multicast Routing Protocol (DVMRP)

A distance-vector-style routing protocol used for routing multicast datagrams through the Internet. DVMRP combines many of the features of RIP with Reverse Path Forwarding (RPF).

Dynamic Host Control Protocol (DHCP)

Provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on the Bootstrap Protocol (BOOTP), adding the capability of automatic allocation of reusable network addresses and additional configuration options.

Extensible Authentication Protocol over LAN (EAPOL)

EAPOL is a client authentication protocol used by this switch to verify the network access rights for any device that is plugged into the switch. A user name and password is requested by the switch, and then passed to an authentication server (e.g., RADIUS) for verification. EAPOL is implemented as part of the IEEE 802.1x Port Authentication standard.

GARP VLAN Registration Protocol (GVRP)

Defines a way for switches to exchange VLAN information in order to register necessary VLAN members on ports along the Spanning Tree so that VLANs defined in each switch can work automatically over a Spanning Tree network.

Generic Attribute Registration Protocol (GARP)

GARP is a protocol that can be used by endstations and switches to register and propagate multicast group membership information in a switched environment so that multicast data frames are propagated only to those parts of a switched LAN containing registered endstations. Formerly called Group Address Registration Protocol.

Generic Multicast Registration Protocol (GMRP)

GMRP allows network devices to register end stations with multicast groups. GMRP requires that any participating network devices or end stations comply with the IEEE 802.1p standard.

Downloaded from www.Manualslib.com manuals search engine

Group Attribute Registration Protocol (GARP)

See Generic Attribute Registration Protocol.

Hot Standby Router Protocol (HSRP)

This protocol allows hosts to connect to a single virtual router and to maintain connectivity even if the actual first hop gateway they are using fails.

IEEE 802.1D

Specifies a general method for the operation of MAC bridges, including the Spanning Tree Protocol.

IEEE 802.1Q

VLAN Tagging—Defines Ethernet frame tags which carry VLAN information. It allows switches to assign endstations to different virtual LANs, and defines a standard way for VLANs to communicate across switched networks.

IEEE 802.1p

An IEEE standard for providing quality of service (QoS) in Ethernet networks. The standard uses packet tags that define up to eight traffic classes and allows switches to transmit packets based on the tagged priority value.

IEEE 802.1s

An IEEE standard for the Multiple Spanning Tree Protocol (MSTP) which provides independent spanning trees for VLAN groups.

IEEE 802.1x

Port Authentication controls access to the switch ports by requiring users to first enter a user ID and password for authentication.

IEEE 802.3ac

Defines frame extensions for VLAN tagging.

IEEE 802.3x

Defines Ethernet frame start/stop requests and timers used for flow control on full-duplex links.

Downloaded from www.Manualslib.com manuals search engine

IGMP Snooping

Listening to IGMP Query and IGMP Report packets transferred between IP Multicast Routers and IP Multicast host groups to identify IP Multicast group members.

IGMP Query

On each subnetwork, one IGMP-capable device will act as the querier — that is, the device that asks all hosts to report on the IP multicast groups they wish to join or to which they already belong. The elected querier will be the device with the lowest IP address in the subnetwork.

Internet Control Message Protocol (ICMP)

A network layer protocol that reports errors in processing IP packets. ICMP is also used by routers to feed back information about better routing choices.

Internet Group Management Protocol (IGMP)

A protocol through which hosts can register with their local router for multicast services. If there is more than one multicast switch/router on a given subnetwork, one of the devices is made the "querier" and assumes responsibility for keeping track of group membership.

In-Band Management

Management of the network from a station attached directly to the network.

IP Multicast Filtering

A process whereby this switch can pass multicast traffic along to participating hosts.

IP Precedence

The Type of Service (ToS) octet in the IPv4 header includes three precedence bits defining eight different priority levels ranging from highest priority for network control packets to lowest priority for routine traffic. The eight values are mapped one-to-one to the Class of Service categories by default, but may be configured differently to suit the requirements for specific network applications.

Downloaded from www.Manualslib.com manuals search engine

Layer 2

Data Link layer in the ISO 7-Layer Data Communications Protocol. This is related directly to the hardware interface for network devices and passes on traffic based on MAC addresses.

Layer 3

Network layer in the ISO 7-Layer Data Communications Protocol. This layer handles the routing functions for data moving from one open system to another.

Link Aggregation

See Port Trunk.

Link Aggregation Control Protocol (LACP)

Allows ports to automatically negotiate a trunked link with LACP-configured ports on another device.

Management Information Base (MIB)

An acronym for Management Information Base. It is a set of database objects that contains information about a specific device.

Multicast Switching

A process whereby the switch filters incoming multicast frames for services for which no attached host has registered, or forwards them to all ports contained within the designated multicast VLAN group.

Network Time Protocol (NTP)

NTP provides the mechanisms to synchronize time across the network. The time servers operate in a hierarchical-master-slave configuration in order to synchronize local clocks within the subnet and to national time standards via wire or radio.

Open Shortest Path First (OSPF)

OSPF is a link-state routing protocol that functions better over a larger network such as the Internet, as opposed to distance-vector routing protocols such as RIP. It includes features such as unlimited hop count, authentication of routing updates, and Variable Length Subnet Masks (VLSM).

Downloaded from www.Manualslib.com manuals search engine

Out-of-Band Management

Management of the network from a station not attached to the network.

Port Authentication

See IEEE 802.1x.

Port Mirroring

A method whereby data on a target port is mirrored to a monitor port for troubleshooting with a logic analyzer or RMON probe. This allows data on the target port to be studied unobstructively.

Port Trunk

Defines a network link aggregation and trunking method which specifies how to create a single high-speed logical link that combines several lower-speed physical links.

Private VLANs

Private VLANs provide port-based security and isolation between ports within the assigned VLAN. Data traffic on downlink ports can only be forwarded to, and from, uplink ports.

Protocol-Independent Multicasting (PIM)

This multicast routing protocol floods multicast traffic downstream, and calculates the shortest-path back to the multicast source network via reverse path forwarding. PIM uses the router's IP routing table rather than maintaining a separate multicast routing table as with DVMRP. PIM - Sparse Mode is designed for networks where the probability of a multicast client is low, such as on a Wide Area Network. PIM - Dense Mode is designed for networks where the probability of a multicast client is high and frequent flooding of multicast traffic can be justified.

Remote Authentication Dial-in User Service (RADIUS)

RADIUS is a logon authentication protocol that uses software running on a central server to control access to RADIUS-compliant devices on the network.

Downloaded from www.Manualslib.com manuals search engine

Remote Monitoring (RMON)

RMON provides comprehensive network monitoring capabilities. It eliminates the polling required in standard SNMP, and can set alarms on a variety of traffic conditions, including specific error types.

Rapid Spanning Tree Protocol (RSTP)

RSTP reduces the convergence time for network topology changes to about 10% of that required by the older IEEE 802.1D STP standard.

Secure Shell (SSH)

A secure replacement for remote access functions, including Telnet. SSH can authenticate users with a cryptographic key, and encrypt data connections between management clients and the switch.

Routing Information Protocol (RIP)

The RIP protocol seeks to find the shortest route to another device by minimizing the distance-vector, or hop count, which serves as a rough estimate of transmission cost. RIP-2 is a compatible upgrade to RIP. It adds useful capabilities for subnet routing, authentication, and multicast transmissions.

Simple Mail Transfer Protocol (SMTP)

A standard host-to-host mail transport protocol that operates over TCP, port 25.

Simple Network Management Protocol (SNMP)

The application protocol in the Internet suite of protocols which offers network management services.

Simple Network Time Protocol (SNTP)

SNTP allows a device to set its internal clock based on periodic updates from a Network Time Protocol (NTP) server. Updates can be requested from a specific NTP server, or can be received via broadcasts sent by NTP servers.

Spanning Tree Protocol (STP)

A technology that checks your network for any loops. A loop can often occur in complicated or backup linked network systems. Spanning Tree detects and directs

Downloaded from www.Manualslib.com manuals search engine

data along the shortest available path, maximizing the performance and efficiency of the network.

Terminal Access Controller Access Control System Plus (TACACS+)

TACACS+ is a logon authentication protocol that uses software running on a central server to control access to TACACS-compliant devices on the network.

Telnet

Defines a remote communication facility for interfacing to a terminal device over TCP/IP.

Transmission Control Protocol/Internet Protocol (TCP/IP)

Protocol suite that includes TCP as the primary transport protocol, and IP as the network layer protocol.

Trivial File Transfer Protocol (TFTP)

A TCP/IP protocol commonly used for software downloads.

User Datagram Protocol (UDP)

UDP provides a datagram mode for packet-switched communications. It uses IP as the underlying transport mechanism to provide access to IP-like services. UDP packets are delivered just like IP packets – connection-less datagrams that may be discarded before reaching their targets. UDP is useful when TCP would be too complex, too slow, or just unnecessary.

Virtual LAN (VLAN)

A Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. A VLAN serves as a logical workgroup with no physical barriers, and allows users to share information and resources as though located on the same LAN.

Virtual Router Redundancy Protocol (VRRP)

A protocol that uses a virtual IP address to support a primary router and multiple backup routers. The backups can be configured to take over the workload if the master fails or to load share the traffic. The primary goal of VRRP is to allow a

Downloaded from www.Manualslib.com manuals search engine

host device which has been configured with a fixed gateway to maintain network connectivity in case the primary gateway goes down.

XModem

A protocol used to transfer files between devices. Data is grouped in 128-byte blocks and error-corrected.

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

INDEX

Symbols

3-31

Numerics

802.1x, port authentication 3-42, 4-74

A

acceptable frame type 3-118, 4-184
Access Control List *See* ACL
ACL
  Extended IP 3-51, 4-82, 4-83, 4-86
  MAC 3-51, 4-82, 4-97, 4-97–4-99
  Standard IP 3-51, 4-82, 4-83, 4-85
Address Resolution Protocol *See* ARP
address table 3-86, 4-159
  aging time 3-88, 4-162
ARP
  configuration 3-183, 4-232
  description 3-182
  proxy 3-182, 4-234
  statistics 3-188, 4-238

B

BOOTP 3-16, 4-227
BPDU 3-89
broadcast storm, threshold 3-78, 4-142

C

Class of Service *See* CoS
CLI, showing commands 4-4
command line interface *See* CLI
community string 2-6, 3-27, 4-108
configuration settings, saving or restoring 2-7, 3-18, 4-61
console port, required connections 2-2
CoS
  configuring 3-124, 4-198
  DSCP 3-132, 3-135, 3-136, 4-206
  IP port priority 3-134, 4-204
  IP precedence 3-131, 4-205
  layer 3/4 priorities 3-130, 4-204
  queue mapping 3-126, 4-201
  queue mode 3-128, 4-199
  traffic class weights 3-128, 4-200

D

default gateway, configuration 3-14, 3-179, 4-229
default priority, ingress port 3-124, 4-198
default settings, system 1-7
DHCP 3-16, 4-227
  address pool 3-158, 4-118
  client 3-14, 4-113, 4-128
  dynamic configuration 2-5
  relay service 3-155, 4-115
  server 3-156, 4-117
Differentiated Code Point Service *See* DSCP
DNS
  default domain name 3-150, 4-130
  displaying the cache 3-154
  domain name list 3-150, 4-128
  enabling lookup 3-150, 4-132
  name server list 3-150, 4-131
  static entries 3-152
Domain Name Service *See* DNS
downloading software 3-17, 4-61
DSCP
  enabling 3-130, 4-206
  mapping priorities 3-132, 3-135, 3-136, 4-207

Downloaded from www.Manualslib.com manuals search engine

DVMRP
configuring 3-234, 4-285
global settings 3-234, 4-285–4-289
interface settings 3-237, 4-289–4-290
neighbor routers 3-239, 4-292
routing table 3-240, 4-292
dynamic addresses, displaying 3-87, 4-160
Dynamic Host Configuration Protocol *See* DHCP

E

edge port, STA 3-98, 3-100, 4-174
event logging 4-41

F

firmware
displaying version 3-11, 4-59
upgrading 3-17, 4-61

G

GARP VLAN Registration Protocol *See* GVRP
gateway, default 3-14, 3-179, 4-229
GVRP
global setting 3-111, 4-194
interface configuration 3-118, 4-195

H

hardware version, displaying 3-11, 4-59
Hot Standby Router Redundancy *See* HSRP
HSRP 3-170, 4-310
authentication 3-173, 4-313
configuration settings 3-170, 4-310
interface tracking 3-173, 4-315
preemption 3-171, 3-172, 4-312
priority 3-171, 3-172, 4-311
timers 3-172, 4-314
virtual address 3-171, 3-173, 4-310
HTTPS 3-34, 4-30
HTTPS, secure server 3-34, 4-30

I

IEEE 802.1D 3-88, 4-164
IEEE 802.1s 4-164
IEEE 802.1w 3-88, 4-164
IEEE 802.1x 3-42, 4-74
IGMP
description of protocol 3-138
groups, displaying 3-144, 4-213, 4-226
Layer 2 3-139, 4-211
Layer 3 3-146, 4-220
query 3-139, 4-214, 4-220
query, Layer 2 3-140, 4-214
query, Layer 3 3-146, 4-220
services, displaying 3-149, 4-226
snooping 3-139, 4-211
snooping, configuring 3-140, 4-211
ingress filtering 3-118, 4-185
IP address
BOOTP/DHCP 3-16, 4-114, 4-227
setting 2-4, 3-14, 4-227
IP port priority
enabling 3-134, 4-204
mapping priorities 3-134, 4-205
IP precedence
enabling 3-130, 4-205
mapping priorities 3-131, 4-206

Downloaded from www.Manualslib.com manuals search engine

IP routing 3-176, 4-235
configuring interfaces 3-180, 4-227
enabling or disabling 3-179, 4-235
status 3-179, 4-235
unicast protocols 3-178
IP, statistics 3-189, 4-238

J

jumbo frame 4-60

L

LACP
configuration 4-150
local parameters 3-74, 4-156
partner parameters 3-77, 4-156
protocol message statistics 4-156
protocol parameters 3-71, 4-150
Link Aggregation Control Protocol *See* LACP
link type, STA 3-98, 3-100, 4-176
logging
syslog traps 4-44
to syslog servers 4-43
log-in, Web interface 3-2
logon authentication 3-30, 4-66
RADIUS client 3-31, 4-67
RADIUS server 3-31, 4-67
TACACS+ client 3-31, 4-70
TACACS+ server 3-31, 4-70
logon authentication, sequence 3-32, 4-66

M

main menu 3-3
Management Information Bases (MIBs) A-3
mirror port, configuring 3-80, 4-147
MSTP 4-164
global settings 3-101, 4-162
interface settings 3-99, 4-163
multicast filtering 3-138, 4-211
multicast groups 3-144, 3-149, 4-213
displaying 3-149, 4-213
static 3-144, 4-212, 4-213
multicast routing 3-231, 4-280
description 3-231
DVMRP 3-234, 4-285
enabling 3-231, 4-282
general commands 4-282
global settings 3-231, 4-282
PIM-DM 3-241, 4-293
routing table 3-232, 4-283
multicast services
configuring 3-145, 4-212
displaying 3-144, 4-213
multicast, static router port 3-142, 4-218, 4-281

O

OSPF 3-206, 4-249
area border router 3-207, 4-254
AS summary route 3-223, 4-255
autonomous system boundary router 3-208, 4-252
backbone 3-210, 4-257
default external route 3-208, 4-252
general settings 3-207, 4-249
normal area 3-210, 4-257
NSSA 3-210, 4-259
redistributing external routes 3-224, 4-256
stub 3-210, 4-258
transit area 3-210, 4-260
virtual link 3-219, 4-260

Downloaded from www.Manualslib.com manuals search engine

P

password, line 4-13
passwords 2-4
  administrator setting 3-30, 4-25
path cost 3-90, 3-98
  method 3-94, 4-167
  STA 3-90, 3-98, 4-167
PIM-DM 3-241, 4-293
  configuring 3-241, 4-293
  global configuration 3-241, 4-294
  interface settings 3-242, 4-294–4-298
  neighbor routers 3-245, 4-300
port authentication 3-42, 4-74
port priority
  configuring 3-124, 4-198
  default ingress 3-124, 4-198
  STA 3-98, 4-173
port security, configuring 3-40, 4-72
port, statistics 3-82, 4-145
ports
  autonegotiation 3-65, 4-138
  broadcast storm threshold 3-78, 4-142
  capabilities 3-65, 4-139
  duplex mode 3-65, 4-137
  flow control 3-65, 4-140
  forced selection on combo ports 3-64, 4-141
  speed 3-65, 4-137
ports, configuring 3-62, 4-136
ports, mirroring 3-80, 4-147
priority, default port ingress 3-124, 4-198
problems, troubleshooting Inde-1
protocol migration 3-101, 4-178
proxy ARP 3-182, 4-234

Q

queue weights 3-128, 4-200

R

RADIUS, logon authentication 3-31, 4-67
rate limits, setting 3-81, 4-149
remote logging 4-44
restarting the system 3-23, 4-22
RIP
  configuring 3-196, 4-240–4-248
  description 3-178
  global settings 3-197, 4-240
  interface protocol settings 3-200, 4-241–4-246
  specifying interfaces 3-199, 4-241
  statistics 3-203, 4-248, 4-249
router redundancy
  HSRP 3-170, 4-310
  protocols 3-163, 4-300
  VRRP 3-164, 4-301
routing table, displaying 3-195, 4-237
RSTP 3-88, 4-164
  global configuration 3-89, 4-164

S

secure shell 3-35, 4-32
Secure Shell configuration 3-35, 4-35, 4-36
serial port
  configuring 4-11
Simple Network Management Protocol *See* SNMP
SNMP 3-26
  community string 3-27, 4-108
  enabling traps 3-28, 4-110
  filtering IP addresses 3-29, 4-111
  trap manager 3-28, 4-109
software
  displaying version 3-11, 4-59
  downloading 3-17, 4-61
Spanning Tree Protocol *See* STA

Downloaded from www.Manualslib.com manuals search engine

specifications, software A-1
SSH, configuring 3-35, 4-35, 4-36
STA 3-88, 4-162
  edge port 3-98, 3-100, 4-174
  global settings, configuring 3-92, 4-163–4-168
  global settings, displaying 3-89, 4-179
  interface settings 3-96, 3-104, 3-107, 4-173–4-178, 4-179
  link type 3-98, 3-100, 4-176
  path cost 3-90, 3-98, 4-173
  path cost method 3-94, 4-167
  port priority 3-98, 4-173
  protocol migration 3-101, 4-178
  transmission limit 3-94, 4-168
standards, IEEE A-2
startup files
  creating 3-19, 4-61
  displaying 3-17, 4-55
  setting 3-17, 4-65
static addresses, setting 3-86, 4-159
static routes, configuring 3-194, 4-236
statistics
  ARP 3-188, 4-238
  ICMP 3-190, 4-238
  IP 3-189, 4-238
  port 3-82, 4-145
  RIP 3-203, 4-248, 4-249
  TCP 3-193, 4-238
  UDP 3-192, 4-238
STP 3-92, 4-164
STP *Also see* STA
system clock, setting 3-24, 4-50
system software, downloading from server 3-17, 4-61

T

TACACS+, logon authentication 3-31, 4-70
time, setting 3-24, 4-50
traffic class weights 3-128, 4-200
trap manager 2-7, 3-28, 4-109
troubleshooting Inde-1
trunk
  configuration 3-67, 4-150
  LACP 3-69, 4-150, 4-151
  static 3-68, 4-151

U

upgrading software 3-17, 4-61
user password 3-30, 4-25, 4-26

V

Virtual Router Redundancy Protocol *See* VRRP
VLANs 3-108–3-121, 4-181–4-193
  adding static members 3-115, 3-116, 4-187
  creating 3-114, 4-182
  description 3-108
  displaying basic information 3-111, 4-195
  displaying port members 3-112, 4-189
  egress mode 3-118, 4-184
  interface configuration 3-117, 4-184–4-188
  private 3-120, 4-193
  protocol 3-121, 4-189
VRRP 3-164, 4-301
  authentication 3-166, 4-302
  configuration settings 3-164, 4-301
  group statistics 3-169, 4-305
  preemption 3-165, 3-166, 4-305
  priority 3-165, 3-166, 4-303
  protocol message statistics 3-168, 4-308
  timers 3-166, 4-304
  virtual address 3-164, 3-166, 4-301

Downloaded from www.Manualslib.com manuals search engine

W

Web interface
  access requirements 3-1
  configuration buttons 3-2
  home page 3-2
  menu list 3-3
  panel display 3-3

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

FOR TECHNICAL SUPPORT, CALL:

From U.S.A. and Canada (24 hours a day, 7 days a week)
(800) SMC-4-YOU; (949) 679-8000; Fax: (949) 679-1481
From Europe : Contact details can be found on
www.smc-europe.com or www.smc.com

INTERNET

E-mail addresses:
techsupport@smc.com
european.techsupport@smc-europe.com
Driver updates:
http://www.smc.com/index.cfm?action=tech_support_drivers_downloads
World Wide Web:
http://www.smc.com
http://www.smc-europe.com

FOR LITERATURE OR ADVERTISING RESPONSE, CALL:

U.S.A. and Canada:	(800) SMC-4-YOU;	Fax (949) 679-1481
Spain:	34-91-352-00-40;	Fax 34-93-477-3774
UK:	44 (0) 1932 866553;	Fax 44 (0) 118 974 8701
France:	33 (0) 41 38 32 32;	Fax 33 (0) 41 38 01 58
Italy:	39 (0) 335 5708602;	Fax 39 02 739 14 17
Benelux:	31 33 455 72 88;	Fax 31 33 455 73 30
Central Europe:	49 (0) 89 92861-0;	Fax 49 (0) 89 92861-230
Nordic:	46 (0) 868 70700;	Fax 46 (0) 887 62 62
Eastern Europe:	34 -93-477-4920;	Fax 34 93 477 3774
Sub Saharian Africa:	216-712-36616;	Fax 216-71751415
North West Africa:	34 93 477 4920;	Fax 34 93 477 3774
CIS:	7 (095) 7893573;	Fax 7 (095) 789 35 73
PRC:	86-10-6235-4958;	Fax 86-10-6235-4962
Taiwan:	886-2-8797-8006;	Fax 886-2-8797-6288
Asia Pacific:	(65) 6 238 6556;	Fax (65) 6 238 6466
Korea:	82-2-553-0860;	Fax 82-2-553-7202
Japan:	81-45-224-2332 ;	Fax 81-45-224-2331
Australia:	61-2-8875-7887;	Fax 61-2-8875-7777
India:	91-22-8204437 ;	Fax 91-22-8204443

If you are looking for further contact information, please visit www.smc.com, www.smc-europe.com, or www.smc-asia.com.

SMC® Networks

38 Tesla
Irvine, CA 92618
Phone: (949) 679-8000

Model Number: SMC8612XL3 F 1.0.1.3
Pub.Number: 150200039900A E102003-R01

Downloaded from www.Manualslib.com manuals search engine